

**This Page Is Inserted by IFW Operations  
and is not a part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Yusaku FUJII

Application No.: To be assigned

Group Art Unit: Unassigned

Filed: March 6, 2002

Examiner: Unassigned

For: ELECTRONIC SETTLEMENT METHOD

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant submits herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-287525


Filed: September 20, 2001.

It is respectfully requested that the applicant be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: March 6, 2002

  
Paul I. Kravetz  
Registration No. 35,230

700 11th Street, N.W., Ste. 500  
Washington, D.C. 20001  
(202) 434-1500

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

Jc972 U.S. PTO  
10/091299  
03/06/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2001年 9月20日

出 願 番 号  
Application Number:

特願2001-287525

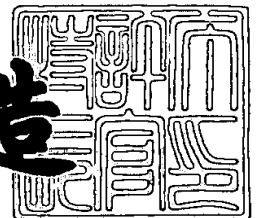
出 願 人  
Applicant(s):

富士通株式会社

2001年12月21日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3111223

【書類名】 特許願

【整理番号】 0151448

【提出日】 平成13年 9月20日

【あて先】 特許庁長官殿

【国際特許分類】 G06F157:00

【発明の名称】 電子決済方法

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 藤井 勇作

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100092978

【弁理士】

【氏名又は名称】 真田 有

【電話番号】 0422-21-4222

【手数料の表示】

【予納台帳番号】 007696

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704824

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子決済方法

【特許請求の範囲】

【請求項 1】 受給者と供給者との間で商取引を行なう際に、該受給者が、該商取引に必要な対価を、決済サービス提供者を介して該供給者に電子的に支払うための電子決済方法であって、

該供給者が、有価データを保持する機能を有するとともに該有価データの受取人を認証するために必要な認証用情報を予め記録された有価データ搬送用電子情報本体を取得して所有するステップと、

該受給者が、該供給者所有の該電子情報本体を取得するステップ（以下、取得ステップという）と、

該受給者が、該決済サービス提供者に対し、該電子情報本体を送信するとともに、前記商取引に必要な対価に対応する価値を有する有価データを該電子情報本体に添付するように依頼するステップ（以下、依頼ステップという）と、

該決済サービス提供者が、該受給者の依頼に応じて、該受給者を認証してから、該有価データを該電子情報本体に添付するステップ（以下、添付ステップという）と、

該電子情報本体と該有価データとからなる有価データ搬送用電子情報が、該決済サービス提供者から該供給者へ返送されるステップ（以下、返送ステップという）と、

該有価データ搬送用電子情報における該有価データの受取希望者が、該電子情報本体に記録された該認証用情報に基づいて、該有価データの受取人本人であると認証された場合に限り、該決済サービス提供者によって、該有価データの所有権が当該受取希望者に移転されるステップ（以下、所有権移転ステップという）を含むことを特徴とする、電子決済方法。

【請求項 2】 正規の受取人以外の利用者によって利用可能な該電子情報本体の機能が、該電子情報本体に有価データを添付・追加する機能に限定されていることを特徴とする、請求項 1 記載の電子決済方法。

【請求項 3】 該決済サービス提供者が、前記添付ステップにおいて該電子

情報本体に有価データを添付・追加する都度、該電子情報本体と追加された有価データとを含む部分に対する電子署名を作成して、該有価データ搬送用電子情報に添付することを特徴とする、請求項 2 記載の電子決済方法。

【請求項 4】 前記添付ステップで該電子情報本体に添付される有価データを所定の公開鍵により暗号化し、該所定の公開鍵に対応する秘密鍵を、該決済サービス提供者および前記受取人のうちの少なくとも一方が管理することを特徴とする、請求項 1 ～請求項 3 のいずれか 1 項に記載の電子決済方法。

【請求項 5】 前記商取引により該供給者から該受給者に受け渡されるべき商品が電子チケットもしくは電子許可証である場合、該供給者が、前記返送ステップで該有価データ搬送用電子情報を受け取ると、該受給者所有の有価データ搬送用電子情報本体に前記の電子チケットもしくは電子許可証を添付し、その電子情報本体を該受給者に送付することを特徴とする、請求項 1 ～請求項 4 のいずれか 1 項に記載の電子決済方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、受給者と供給者との間で商取引を行なう際に、受給者が、商取引に必要な対価を、決済サービス提供者を介して供給者に電子的に支払うための電子決済方法に関する。

近年、インターネットの普及により、インターネット上での商取引が活発に行なわれるようになってきている。これに伴い、企業間（B2B）のみならず、消費者間（C2C）でも、ネットオークションに代表されるように、金銭授受を伴う商取引をインターネット上で行なう場面が増えてきた。ところが、インターネット上では取引相手の姿が見えず、利用者には常に詐欺の不安が付きまとう。また、クレジットカード決済などでは、単純な人為的ミスにより誤った額が引き落されてしまうおそれもある。本発明は、これらの不安を解消するための、インターネット上での新たな金銭の授受方法（電子決済方法）に関するものである。

【0 0 0 2】

【従来技術】

一般に、インターネット上での決済方式としては、以下のような方式〔a1〕～〔a3〕が用いられている。なお、以下の説明では、顧客に対して商品や何らかのサービスを供給する側（店舗等）のことを供給者（または供給側）といい、この供給者と商取引を行ない対価を支払って供給者から商品やサービスを供給される側（前記顧客）のことを受給者（または受給側）という。また、受給者が商取引に必要な対価を供給者に支払う際に受給者と供給者とを仲介する業者のことを決済サービス提供者（または決済サービス側）という。

【0003】

〔a1〕クレジットカード方式

クレジットカード方式では、受給側が、供給側にクレジットカード番号、有効期限などを通知し、クレジットカード会社（決済サービス提供者）を通して、代金（対価）を供給側に支払う。供給側は、受給側から通知されたクレジットカード番号をCAT（Credit Authorization Terminal）端末に入力し、クレジットカード会社取引内容を通知する。

【0004】

〔a2〕プリペイドカード（電子マネー）方式／電子小切手方式

受給側は、第三者の決済サービス側と予め契約し、決済サービス側に適当な金額の現金を支払うことにより、プリペイドカード番号や電子小切手等を予め入手しておく。そして、受給側が供給側から商品やサービスを購入する際に、受給側は、決済サービス側から与えられたプリペイドカード番号や電子小切手等を供給側に送信することにより、代金（対価）を供給側に支払う。供給側は、受給側から送信されたプリペイドカード番号や電子小切手等を決済サービス側に送信し、決済サービス側から所定の現金を受け取る。

【0005】

〔a3〕インターネットバンキング（オンラインバンキング）による振込み

受給側が供給側の指定口座に現金を振り込むことにより、代金（対価）を供給側に支払う。この振込み作業を、インターネットバンキングサービスを用いてオンライン上で行なった場合、インターネット上で金銭の授受は完結することになる。

【0006】

一方、上述のような方式によりインターネット上で決済を行なうことはできるが、インターネット上での決済に際しては、インターネット固有の匿名性のために詐欺の心配が常に付きまとう。そこで、近年、供給側と受給側との間に相互に信頼関係が無い場合であっても安全な商取引を行なうことが可能なエスクローサービスが提供されており、このエスクローサービスと上述した決済方式とを組み合わせることも行なわれている。

【0007】

ここで、エスクローサービスとは、互いに信用の置けない二者間で商取引を行なう際、信用の置ける第三者が一時的に現金を預かることで安全な商取引を保証するサービスのことである。エスクローサービスは、一般に以下の手順（b1）～（b6）で行なわれる。

（b1）受給側が供給側に商品・サービス・許可証等を発注する。

（b2）受給側がエスクローサービス提供者に現金を預ける。

（b3）供給側が受給側に受注品を発送する。

（b4）受給側が受注品を確認し、所望品であるかどうかをエスクローサービス提供者に通知する。

（b5）エスクローサービス提供者は、所望品である旨の通知を受給側から受けると、預かっていた現金を供給側に渡す。

（b6）供給側と受給側との間でトラブルが発生した場合は、そのトラブルが解決するまでエスクローサービス提供者が現金を預かっておく。

【0008】

【発明が解決しようとする課題】

しかしながら、上述した決済方式では、以下のような課題がある。

〔c1〕クレジットカード方式の課題

〔c1-1〕供給側の社員の不正

受給者がWWW（World Wide Web）でオンラインショッピングを行なっても、多くの中小企業では、そのオンラインショッピングの決済途中に人手が介入することが多い。つまり、多くの中小企業ではクレジットカード決済は自動化されて



おらず、従業員が、自らの手で、顧客（受給側）から送信されてきたクレジットカード番号、有効期限、支払額などを手元のＣＡＴ端末に入力して決済を行なっている。つまり、クレジットカード番号や有効期限などは、従業員にさらされる環境となっていることが多く、社員が不正を働けば、クレジットカード番号は簡単に盗まれたり漏れたりするおそれがある。

【 0 0 0 9 】

〔 c 1 - 2 〕 供給側のＣＡＴ端末操作ミス

上述した通り、多くの中小企業では、従業員がＣＡＴ端末を操作して決済を行なっているため、その際、支払額について操作ミスをする可能性がある。万一、操作ミスのために、実際に支払うべき額よりも大きい値が支払額が入力されてしまうと、必要以上の現金が受給側の口座から引落されてしまうおそれがある。

【 0 0 1 0 】

〔 c 1 - 3 〕 クレジットカード番号の盗聴／盗難

クレジットカード番号がインターネット上を流れるため、常に盗聴／盗難の危険にさらされることになる。つまり、受給者がクレジットカードを利用して支払いを行なう場合、その操作が盗聴される危険性がある。WWW上に入力したクレジットカード番号などが盗聴されると、勝手に口座から現金が引き出されるおそれがある。そこで、近年では、主にSSL（Secure Socket Layer）と呼ばれる暗号化プロトコルを用いて盗聴／盗難を阻止している。また、SET（Secure Electronic Transaction）と呼ばれる電子商取引専用の通信手順を採用することも考えられる。しかし、この通信手順を採用するためには、供給側や決済サービス側に新たに専用の複雑なシステムを構築しなければならず、コストがかかる上、使用し難いため、SETはあまり普及していない。

【 0 0 1 1 】

〔 c 2 〕 プリペイドカード（電子マネー）方式／電子小切手方式の課題

〔 c 2 - 1 〕 カード番号や電子小切手データの盗聴・盗難

クレジットカード方式と同じく、カード番号や電子小切手データがインターネット（WWW）上を流れるので、常に盗聴・盗難の危険にさらされる。

〔 c 2 - 2 〕 供給側の社員の不正

カード番号や電子小切手は、供給側を介して決済サービス側に送られるため、供給側の社員が不正を働けばカード番号や電子小切手が盗まれ悪用されるおそれがある。

#### 【 0 0 1 2 】

##### 〔 c 2 - 3 〕 二重使用

電子マネーや電子小切手は、それ自身、単なるデジタルデータ（データ列）であるため、パーソナルコンピュータ等の端末上で極めて簡単にコピーできる。つまり、有価データである電子小切手をユーザが簡単に複製できてしまう。複製物はオリジナルとの区別がつかないため、使用前の電子マネーや電子小切手を複製し、二重に使用することが可能になってしまう。そこで、決済サービス側は、電子小切手の二重使用を防止するためのシステムを構築する必要がある。二重使用防止システムとしては、例えば、次のようなものがある。決済サービス側において、過去に現金化された電子小切手の管理番号を全てデータベースに保存しておき、電子小切手の現金化を行なう際に、その電子小切手の管理番号がそのデータベースに存在しているか否かを検索して調べ、データベースに存在していない場合に限り、その電子小切手の現金化を行なう。このようなシステムでは、現金化済みの電子小切手の管理番号を半永久的に保存し続けなければならない、データベースに保存されるべき管理番号のデータ量は膨大なものとなる。従って、極めて大容量の記憶装置が必要であり、システムの構築に多大なコストを要することになる。

#### 【 0 0 1 3 】

##### 〔 c 2 - 4 〕 プライバシーの侵害

インターネット上での取り引きに電子小切手を用いた場合、顧客（受給側）の金の使用履歴が残ってしまうことがある。即ち、電子小切手の発行に際しては、通常、支払人（受給側）の署名が使用されるため、現金の匿名性を保持できず、受給側の支払い用途が外部に漏れ受給側のプライバシーが侵害されるおそれがある。

#### 【 0 0 1 4 】

##### 〔 c 3 〕 インターネットバンキング（オンラインバンキング）による振込み

## 〔c 3 - 1〕面倒な振込み確認作業

受給側がオンラインバンキングを利用した振込みにより商取引の決済を行なう場合、供給側は、金融機関からの振込み通知を確認した後、商品の発送などを行なう。振込み処理を使用した場合、振込みに時間がかかったり（現状では午後3時以降の振込みは翌日扱い等）、供給側が銀行から振込みされた旨の連絡を待つなどして、実際の商品発送まで時間がかかる。また、金融機関からの振込み通知は、オンラインではなく、一般に非電子化情報（例えばファクシミリによる通知等）によって振込み通知が行なわれるため、供給側は受給側の振込み完了を直ちに確認することができない。従って、供給側にとって振込み確認作業が面倒であり、振込み通知の待ち時間が、商取引の作業の効率を低下させる要因になっている。つまり、振込み確認作業を完全に自動化することができず、商品の発送までに時間がかかってしまう。

## 【0015】

## 〔c 3 - 2〕供給側の詐欺

インターネットは匿名性が高く、一般に取引相手の信用確認が非常に難しい。そのため、詐欺が発生しやすく、詐欺が発生した場合は、犯人を追跡することが極めて難しい。従って、受給側が供給側の口座に所定の支払額の現金を振り込んだ後に供給側が詐欺を働いていることが判明しても、受給側は、現金を取り返すことができない場合が多い。

## 【0016】

〔c 3 - 3〕インターネットバンキングを使用するためのパスワードの盗聴／盗難

インターネットバンキング利用のためのパスワードがインターネット（WWW）上を流れるので、前述したクレジットカード番号、プリペイドカード番号や電子小切手データと同様、常に盗聴／盗難の危険にさらされる。

## 【0017】

## 〔c 4〕エスクローサービスの利用

エスクローサービスは、前述した通り、安全な取引の手順を提供するものである。このようなエスクローサービスの提供を受ける場合、受給側は、この受給側

と供給側とを仲介するエスクローサービス提供会社に所定の支払額を支払う必要がある。その支払に際し上述した決済方式〔a 1〕～〔a 3〕を用いると、結局、上述と同様の課題〔c 1〕～〔c 3〕が生じることになる。

【0018】

従来の決済方式では、上述した盗聴、詐欺、プライバシーの侵害などの不安が利用者に付きまとう。これが、近年、オンラインショッピングサイトが増えつつあるにもかかわらず未だに活発に利用されていないことの主要因であると考えられる。従って、供給側からは、上述のような不安を解消し受給者がオンラインショッピングサイト等を安心して利用できるようにし、オンラインショッピングサイト等を利用した商取引の活発化、ひいてはオンラインショッピングサイト等での売上向上を実現することが望まれている。

【0019】

また、従来の決済方式（特に電子マネー方式や電子小切手方式）では、二重使用防止システムの構築に多大なコストを要することになる。このため、決済サービス側からは、二重使用防止システムを簡易かつ安価に構築することのできる電子決済方法の開発が強く要望されている。

本発明は、このような課題に鑑み創案されたもので、商取引の手順を工夫することにより受給者が安心して決済を行なえるようにして、インターネット等を利用した電子商取引の活発化、ひいては売上向上を実現するとともに、二重使用防止システムを簡易かつ安価に構築できるようにした、電子決済方法を提供することを目的とする。

【0020】

【課題を解決するための手段】

上記目的を達成するために、本発明の電子決済方法（請求項1）は、受給者と供給者との間で商取引を行なう際に、該受給者が、該商取引に必要な対価を、決済サービス提供者を介して該供給者に電子的に支払うための電子決済方法であって、該供給者が、有価データを保持する機能を有するとともに該有価データの受取人を認証するために必要な認証用情報を予め記録された有価データ搬送用電子情報本体を取得して所有するステップと、該受給者が、該供給者所有の該電子情

報本体を取得するステップ（以下、取得ステップという）と、該受給者が、該決済サービス提供者に対し、該電子情報本体を送信するとともに、前記商取引に必要な対価に対応する価値を有する有価データを該電子情報本体に添付するように依頼するステップ（以下、依頼ステップという）と、該決済サービス提供者が、該受給者の依頼に応じて、該受給者を認証してから、該有価データを該電子情報本体に添付するステップ（以下、添付ステップという）と、該電子情報本体と該有価データとからなる有価データ搬送用電子情報が、該決済サービス提供者から該供給者へ返送されるステップ（以下、返送ステップという）と、該有価データ搬送用電子情報における該有価データの受取希望者が、該電子情報本体に記録された該認証用情報に基づいて、該有価データの受取人本人であると認証された場合に限り、該決済サービス提供者によって、該有価データの所有権が当該受取希望者に移転されるステップ（以下、所有権移転ステップという）とを含むことを特徴としている。

#### 【 0 0 2 1 】

なお、正規の受取人以外の利用者によって利用可能な該電子情報本体の機能を、該電子情報本体に有価データを添付・追加する機能に限定してもよく（請求項 2）、その際、該決済サービス提供者が、前記添付ステップにおいて該電子情報本体に有価データを添付・追加する都度、該電子情報本体と追加された有価データとを含む部分に対する電子署名を作成して、該有価データ搬送用電子情報に添付してもよい（請求項 3）。

#### 【 0 0 2 2 】

また、前記添付ステップで該電子情報本体に添付される有価データを所定の公開鍵により暗号化し、該所定の公開鍵に対応する秘密鍵を、該決済サービス提供者および前記受取人のうちの少なくとも一方が管理してもよい（請求項 4）。

さらに、前記商取引により該供給者から該受給者に受け渡されるべき商品が電子チケットもしくは電子許可証である場合、該供給者が、前記返送ステップで該有価データ搬送用電子情報を受け取ると、該受給者所有の有価データ搬送用電子情報本体に前記の電子チケットもしくは電子許可証を添付し、その電子情報本体を該受給者に送付してもよい（請求項 5）。

【 0 0 2 3 】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態を説明する。

〔 1 〕 第 1 実施形態の説明

〔 1 - 1 〕 第 1 実施形態の電子決済方法を適用されるシステムの基本構成

図 1 は本発明の第 1 実施形態としての電子決済方法を適用されるシステムの構成および同方法の手順を説明するための図である。

【 0 0 2 4 】

まず、図 1 を参照しながら、第 1 実施形態の電子決済方法を適用されるシステムの基本的な構成について説明する。

図 1 に示すように、第 1 実施形態の電子決済方法を適用されるシステムは、少なくとも、商品やサービスなどの価値のあるものを供給する供給側（供給者）としての店舗 2 と、この供給側 2 から商品やサービスなどを受け対価を支払う受給側（受給者）としての顧客 1 と、これらの顧客 1 と店舗 2 との間の商取引を仲介する決済サービス側（決済サービス提供者）としての決済サービス会社 3 とから構成される。本実施形態の電子決済方法は、上述のようなシステムにおいて、顧客 1 が、商取引に必要な対価を、決済サービス会社 3 を介して店舗 2 に電子的に支払うための方法である。ここで、決済サービス会社 3 は、例えば、銀行等の金融機関や、クレジットカード会社である。なお、図 1 では、店舗 2 と決済サービス会社 3 との間に顧客 1 以外に承認者（第三者、承認者端末） 4 が示されているが、この承認者 4 については後述する。

【 0 0 2 5 】

ここでいう顧客 1 とは、実際には、顧客によって使用されるパーソナルコンピュータ等の端末（受給側端末）であり、店舗 2 とは、店舗側にそなえられたサーバ（供給側サーバ）であり、決済サービス会社 3 とは、決済サービス会社側にそなえられたサーバ（決済サービス側サーバ）である。そして、これらの端末 1 およびサーバ 2, 3 の相互間は、データ交換手段によって情報転送可能に接続されている。

【 0 0 2 6 】

データ交換手段は、端末 1 およびサーバ 2, 3 の相互間で情報転送を行なうもので、このデータ交換手段としては、有線通信手段および無線通信手段の両方またはいずれか一方を用いてもよいし、情報を記録した可搬型記録媒体を顧客 1, 店舗 2 および決済サービス会社 3 の間でやり取りする手段を用いてもよい。

## 【 0 0 2 7 】

ここで、有線通信手段は、例えば、電話線、ケーブルテレビ線、電力線、音楽配信線、LAN (Local Area Network), WAN (Wide Area Network) 等であり、無線通信手段は、例えば、携帯電話、PHS (Personal Handyphone System), 無線 LAN 等である。また、可搬型記録媒体は、例えば IC (Integrated Circuit) カード、メモリカード等の電子記録媒体や、磁気カード、磁気ディスク等の磁気記録媒体や、MO (Magneto Optical disk), DVD (Digital Versatile Disk) / CD (Compact Disk) -R (Recordable) / RW (ReWritable) 等の光磁気記録媒体や、バーコード、活字等の印刷物等である。有線通信手段や無線通信手段を用いた場合には、即時性が高くなり、快適に電子決済システムを利用することができる一方、可搬型記録媒体を用いた場合には、オフラインでも電子決済を使用でき、通信環境を整える必要が無くなる。

## 【 0 0 2 8 】

## 〔 1 - 2 〕 電子財布の構成および機能

本実施形態の電子決済方法では、顧客 1, 店舗 2 および決済サービス会社 3 の間において上述したデータ交換手段を用い電子財布 C をやり取りすることによって、顧客 1 が、商取引に必要な対価を店舗 2 に電子的に支払うことを基本的な特徴としている。

## 【 0 0 2 9 】

この電子財布 C の構成や機能について、以下に説明する。

本実施形態の電子財布 (有価データ搬送用電子情報) C は、電子財布本体 (有価データ搬送用電子情報本体) C 0 を核として構成され、顧客 1, 店舗 2 および決済サービス会社 3 の相互間において、決済サービス会社 3 で電子データとして発行された有価データを転送するための電子データである。

## 【 0 0 3 0 】

電子財布本体C0は、決済サービス会社3から店舗（供給者）2に対して発行され、店舗2によって所有されるもので、有価データを保持する機能を有する電子データである。この電子財布本体C0には、有価データの受取人（現金化実行者、換金実行者）を認証するために必要な認証用情報が予め記録されている。本実施形態において、有価データの受取人は、電子財布本体C0の所有者である店舗（供給者）2としているが、所有者以外に、店舗（供給者）2を管理する管理者であってもよい。

【0031】

電子財布本体C0に記録される認証用情報は、例えば、

（A1）有価データの受取希望者の認証時にその受取希望者から取得された認証対象情報（パスワード、バイオメトリクス情報等）と照合されるべき受取人認証情報、あるいは、

（A2）発行元である決済サービス会社3によって付与された電子財布本体C0固有の識別子である。

【0032】

認証用情報が電子財布本体C0固有の識別子である場合、有価データの受取希望者の認証時には、その受取希望者から取得された認証対象情報を登録受取人認証情報と照合すべく、その登録受取人認証情報を識別子に基づいて読み出すことになる。このため、識別子と、その識別子を付与された電子財布本体C0について予め登録された受取人認証情報とを対応付けて管理する必要がある。そこで、上述のような識別子と受取人認証情報との対応関係は、テーブル形式で決済サービス会社3におけるデータベースに保存されて管理されるか、もしくは、可搬型記録媒体に記録されて管理される。

【0033】

なお、上記可搬型媒体としては、例えば、ICカード、メモ리카ード等の電子記録媒体や、磁気カード、磁気ディスク等の磁気記録媒体や、MO、DVD/CD-R/RW等の光磁気記録媒体や、バーコード等の印刷物等が用いられる。

また、受取人認証情報（認証対象情報）としては、パスワード（文字列）を用



いてもよいし、指紋、声紋、虹彩、眼底網膜血管網、顔画像、掌紋、指形、掌形、動的署名、静脈血管網、キーストロック等のバイオメトリクス情報を用いてもよい。

【 0 0 3 4 】

一方、電子財布本体 C 0 には、この電子財布本体 C 0 の発行元（発行者）に関する発行元情報（発行者情報）が、その内容を外部から誰でも確認可能に予め記録されている。つまり、電子財布 C を受け取った顧客 1、供給者 2 や承認者 4 は、端末上で、電子財布本体 C 0 における発行元情報の内容を参照して確認することができるようになっている。本実施形態では、電子財布本体 C 0 の発行元は、決済サービス会社 3 であるので、例えば、会社名（金融機関名）などが発行者情報として記録される。これにより、その電子財布本体 C 0 に後述するごとく添付される有価データを必ず現金化できることが保証され、利用者（顧客 1 や供給者 2 など）に安心感を与えることができる。このとき、発行者情報を改竄できないように、発行者情報に電子署名を付してもよい。

【 0 0 3 5 】

また、電子財布本体 C 0 には、後述するごとく、顧客 1 からの依頼に応じて決済サービス会社 3 により電子小切手等の有価データが添付・追加されるようになっている。このとき、有価データは、その内容を外部から誰でも確認可能に電子財布本体 C 0 に添付される。つまり、電子財布 C を受け取った顧客 1、供給者 2 や承認者 4（第三者）は、端末上で、電子財布本体 C 0 に添付された有価データの内容（電子小切手の額面等）を参照して確認できるようになっている。

【 0 0 3 6 】

さらに、本実施形態では、正規の受取人以外の利用者によって利用可能な電子財布 C の機能は、その電子財布 C（電子財布本体 C 0）に有価データを添付・追加する機能のみに限定されている。従って、正規の受取人以外の利用者は、有価データを電子財布 C に追加することしかできず、電子財布 C に添付された有価データの取出し（換金／出金）を行なえないようになっている。つまり、有価データの受取希望者が、決済サービス会社 3 において、電子財布本体 C 0 に予め登録された受取人本人であることが認証されない限り、有価データの現金化／換金を

行なえないようになっている。なお、電子財布 C（電子財布本体 C 0）への有価データの追加・保存手法については、図 4～図 8 を参照しながら後述する。

#### 【 0 0 3 7 】

##### 〔 1 - 3 〕 第 1 実施形態の電子決済方法の手順

次に、上述のごとく構成されたシステムや電子財布 C を用いて実行される、本発明の第 1 実施形態としての電子決済方法の手順について、図 1 に示す矢印（ステップ、手順）A 1 1～A 2 5 を参照するとともに図 2～図 8 を参照しながら説明する。なお、図 2 および図 3 はそれぞれ第 1 実施形態の電子財布本体に対する電子署名付与手法／情報追加手法の第 1 例および第 2 例を説明するための図、図 4 は第 1 実施形態における電子財布への有価データの追加・保存手法の第 1 例を説明するための図、図 5 および図 6 はいずれも第 1 実施形態における電子財布への有価データの追加・保存手法の第 2 例を説明するための図、図 7 および図 8 はいずれも第 1 実施形態における電子財布への有価データの追加・保存手法の第 3 例を説明するための図である。

#### 【 0 0 3 8 】

図 1 では、受給側（顧客）1 が、供給側（店舗）2 からオンラインショッピング等で物品（もしくは何らかのサービス）を購入するとき、決済サービス会社（金融機関）3 を介して、その物品の代金（対価）を支払う手順（電子決済手順）A 1 1～A 2 5 が示されている。

#### 【 0 0 3 9 】

##### 〔 1 - 3 - 1 〕 電子財布の発行手続

まず、受給側 1 から代金を受け取る側である供給側 2 は、受給側 1 との取り引きに先立って、代金を受け取るための電子財布本体（有価データ搬送用電子情報本体）C 0 を、決済サービス会社 3 から発行してもらう（矢印 A 1 1, A 1 2 参照）。電子財布本体 C 0 は、供給側 2 が決済サービス側 3 と契約することにより作成され発行される。

#### 【 0 0 4 0 】

つまり、電子財布本体 C 0 を作成したい旨（発行依頼）が供給側 2 から決済サービス側 3 に伝えられると（矢印 A 1 1 参照）、決済サービス会社 3 は、有価デ

ータの受取人である供給者 2 の本人認証データ（所有者認証情報／受取人認証情報；実際にはパスワード等の文字列もしくは指紋データ等のバイオメトリクス情報）を取得し、この本人認証データを認証用情報として記録された電子財布本体 C 0（図 2～図 8 参照）を作成する。このとき、電子財布本体 C 0 には、発行者である決済サービス会社 3 の情報を含む発行者情報も記録される（図 2～図 8 参照）。発行者情報は、例えば決済サービス会社 3 の社名や発行日である。このように認証用情報や発行者情報を記録された電子財布本体 C 0 の全体に対しては、さらに、決済サービス会社（発行者） 3 による電子署名を添付することが好ましい（図 2 や図 3 参照）。

#### 【 0 0 4 1 】

なお、前述した通り、電子財布本体 C 0 に記録される認証用情報は、供給者 2 から取得された本人認証データ（所有者認証情報／受取人認証情報）そのものであってもよいし、電子財布本体 C 0 に付与された固有の識別子であってもよい。ただし、識別子を認証用情報として用いる場合、識別子と本人認証データとの対応関係は、決済サービス側 3 で保持・管理されるか、もしくは、可搬型記録媒体に記録された状態で電子財布本体 C 0 の所有者（供給側 2）により管理される。

#### 【 0 0 4 2 】

そして、決済サービス会社 3 は、作成された電子財布本体 C 0 を供給側 2 に対して発行・送付する（矢印 A 1 2 参照）。その際、供給側 2 は、決済サービス会社 3 から発行された電子財布本体（実体は無体物の単なる電子データ） 3 を、可搬記録媒体に記憶させて持ち帰るか、もしくは、有線通信手段／有線通信手段を通じて電子メール等により送信してもらう。このようにして、供給側 2 は、予め電子財布本体 C 0 を取得して所有する。

#### 【 0 0 4 3 】

この後、供給側 2 は、オンラインショッピングを開設する際に、その電子財布本体 C 0 を顧客 1 が自由に取得できるように、商品情報を例えば WWW 上のホームページ等で一般公開する。これにより、顧客 1 には、そのホームページから電子財布本体 C 0 を随時ダウンロードして取得することのできる環境が提供されることになる（矢印 A 1 5 参照）。電子財布本体 C 0 を、WWW 上で公開するほか

に雑誌や広告等で一般公開してもよい。

【 0 0 4 4 】

このように電子財布本体 C 0 を一般公開しておくこと、顧客 1 は、必要なときに電子財布本体 C 0 を取得し、商品等の発注処理を行なうことができる。また、供給側 2 が各顧客 1 と個別に対応をとって電子財布本体 C 0 を顧客 1 に与える必要がなくなる。

なお、電子財布本体 C 0 を、IC カード、メモリカード、磁気カード、磁気ディスク、MO、DVD / CD-R / RW、バーコード等の可搬型記録媒体に記録して顧客 1 に配布することによって、電子財布本体 C 0 を顧客 1 に提供してもよい。

【 0 0 4 5 】

〔 1 - 3 - 2 〕 預金口座の開設手続

一方、顧客（受給側）1 は、商品の購入に先立って、電子財布 C に対し自由に入金できるように、つまり電子財布本体 C 0 に自由に有価データを添付できるように決済サービス会社 3 と契約し預金口座を開設する。このとき、顧客 1 が、預金口座を開設したい旨を決済サービス会社 3 に通知すると（矢印 A 1 3 参照）、決済サービス会社 3 は、顧客 1 の預金口座を開設した後、顧客 1 についての本人認証データ（顧客認証情報）を取得・作成するとともに、顧客識別情報（顧客 ID）を発行し、これらの顧客 ID および本人認証データと預金口座とを対応付けて保持する。

【 0 0 4 6 】

本人認証データとしては、顧客 1 から取得された指紋データ等のバイオメトリクス情報や、顧客 1 によって指定された、もしくは、決済サービス会社 3 によって作成されたパスワード等の文字列が用いられる。これ以外に、本人認証データとしては、特定の端末に関する情報（特定端末情報）を用いることもできる。例えば IP（Internet Protocol）アドレスや携帯電話を特定端末情報として用いることにより、特定のパーソナルコンピュータや特定の携帯電話による入金を許可するようにしてもよい。

【 0 0 4 7 】

そして、決済サービス会社 3 は、パスワード認証を行なう場合には顧客 I D および本人認証データ（パスワード）の両方を、バイオメトリクス認証や特定端末情報による認証を行なう場合には顧客 I D のみを顧客 1 に通知する（矢印 A 1 4 参照）。このとき、顧客 1 は、顧客 I D および本人認証データを、自分で記憶したり可搬型記録媒体に記録したりして持ち帰ってもよいし、決済サービス会社 3 から電子メール等で自宅に送ってもらってもよい。この後、顧客 1 は、電子財布 C に対し自由に入金ができるように、ある程度の現金を開設した預金口座に入金しておく。

#### 【 0 0 4 8 】

なお、以上説明した手順 A 1 1 ～ A 1 4 による手続は、本実施形態による電子決済サービスを利用するに先立って完了されるべきことであるが、この手続を一旦完了しておけば、顧客 1 がオンラインショッピングに伴う電子決済を行なう度に上述した手順 A 1 1 ～ A 1 4 を行なう必要はない。つまり、手順 A 1 1 ～ A 1 4 による手続の完了後、オンラインショッピングに伴う代金の電子決済は、以下に説明する、A 1 5 以降の手順に従って行なわれることになる。

#### 【 0 0 4 9 】

##### 〔 1 - 3 - 3 〕 電子財布への入金処理

顧客 1 は、オンラインショッピングで、店舗 2 から購入する商品あるいはサービス（以下、商品等という）を決定すると、まず、店舗 2 所有の電子財布 C（電子財布本体 C 0）を、例えば WWW を通じてダウンロードするなどして取得する（取得ステップ；矢印 A 1 5 参照）。なお、商品等としては、通常の物品のほか、各種サービスの利用権利や、入場チケットなどの許可証（電子チケット、電子許可証など）が含まれる。

#### 【 0 0 5 0 】

そして、顧客 1 は、取得した電子財布 C に購入商品等の代金（購入商品等の対価に対応する価値を有する有価データ）を入金するために、その電子財布 C を、電子メールにより、もしくは、WWW を通じて決済サービス会社 3 に送るとともに、決済サービス会社 3 に対し、入金依頼つまり有価データの添付依頼を行なう（矢印 A 1 6 参照；依頼ステップ）。

## 【0051】

このとき、顧客1は、電子財布Cとともに、電子財布Cに入金すべき代金の金額と、前記手順A13、A14によって得られた顧客IDと、顧客認証情報（パスワードもしくはバイオメトリクス情報）とを決済サービス会社3に送信・通知する。また、顧客1が後述するエスクローサービス（矢印A22、A23参照）を利用したい場合には、電子財布Cの送信時に、その旨を決済サービス会社3に通知する。

## 【0052】

一方、決済サービス会社3は、電子財布Cへの入金処理を顧客1から依頼されると、まず、顧客1から受け取った顧客IDおよび顧客認証情報に基づいて、入金依頼主の顧客1が決済サービス会社3と正当な契約関係にあるか否か（決済サービス会社3によって開設された預金口座の契約者であるか否か）を判定する。顧客1が正当な顧客であると判定された場合、決済サービス会社3は、顧客1の預金口座から指定金額（商品等の代金）を減額し、その金額に相当する価値を有する電子小切手等の有価データを生成・発行し、その有価データを電子財布本体C0に添付することにより電子財布Cに入金する（添付ステップ）。

## 【0053】

決済サービス会社3が有価データを電子財布本体C0に添付すべく顧客1の預金口座から指定金額を減額する際には、所定の確認先に対し、預金口座からの減額処理つまり有価データの添付処理を実行してもよいかどうかの確認（矢印A17、A18参照）を行なうことが好ましい。確認先（確認の連絡先）としては、預金口座の契約者である顧客1や、予め登録された顧客1以外の第三者（例えば図1に示す承認者4など）が考えられる。また、確認先は、決済サービス会社3側で予め登録されていてもよいし、電子財布C（電子財布本体C0）に予め記録されていてもよい。電子財布C（電子財布本体C0）への確認先の記録は、例えば、顧客1の端末上で行なう。つまり、電子財布本体C0に確認先を追加情報として追加する。その際、電子財布本体C0と確認先情報とに対する電子署名を作成し、電子情報本体C0に添付することにより、確認先情報の改竄を防止する。なお、確認先に対する確認は、例えば、電話（携帯電話、PHSを含む）、ファ

クシミリ、郵便、電子メール、リモートプリント、専用通信ソフトウェア、WWW、メッセージソフトのいずれかを用いて実行される。

【0054】

即ち、決済サービス会社3は、有価データの入金処理を実行してもよいかどうかの問い合わせを確認先（預金口座の所有者等；図1では顧客1）に対して行ない（矢印A17参照）、その問い合わせに対する確認先からの回答（矢印A18）で承認を得られなければ、有価データの生成・発行および電子財布Cへの入金を行なわない。従って、決済サービス会社3は、入金処理の承認を確認先から得られた場合のみ、有価データの生成・発行および電子財布Cへの入金を行なう。

【0055】

なお、有価データの入金処理を実行してもよいかどうかの確認は、顧客1以外の第三者に行なってもよい。例えば図1に二点鎖線の矢印A17'、A18'で示すごとく、決済サービス会社3は、顧客1の商品購入を管理する承認者4から入金処理の承認を行なってもよい。承認者4は、例えば、顧客1の商品購入を管理する管理者（顧客1の仕事上の上司等）や、顧客1が他人の預金口座の現金により入金処理を行なう場合にその預金口座の開設者などである。

【0056】

このように、現金の移動（有価データの生成・添付）を行なう際に、その確認を行なうことにより、安全性を高めることができる。例えば、手順A16で顧客1が決済サービス会社3へ電子財布Cなどを送信する際に、万一、犯罪者により顧客IDおよび顧客認証情報が盗まれ、且つ、その犯罪者が自分の電子財布を所有していると、顧客1はその犯罪者に金を取られるおそれがある。つまり、犯罪者が、盗んだ顧客IDおよび顧客認証情報とともに自分の電子財布を決済サービス会社3に送ると、決済サービス会社3は、犯罪者によって指定された金額に相当する有価データを生成し、犯罪者の電子財布に記録してしまう。このような場合、手順A17、A18やA17'、A18'として上述したごとく、預金口座の減額処理を確認する機能がそなえられていれば、犯罪者が不正に現金を移動しようとしている事実が事前に判明し、顧客1や決済サービス会社3は、そのような不正行為を未然に防ぐことができる。

【0057】

このとき、電話（携帯電話，PHSを含む），ファクシミリ，電子メール等の一般的な手段を用いて確認手続を行なうことにより、その確認手続は利用者に受け入れられやすくなる。

また、携帯電話，PHS等を用いれば、預金口座所有者等の確認先に対する確認を素早く行なうことができる。

さらに、確認の連絡先を決済サービス会社3側で保持しておけば、犯罪者が連絡先を書き換えて不正な現金移動を発覚しないようにすることが困難になる。一方、確認の連絡先を電子財布Cに記録しておけば、電子財布Cを使用する度に現金移動の確認先を柔軟に変更することができる。

【0058】

上記添付ステップにおいて決済サービス会社3が有価データを発行した場合、その有価データには、決済サービス会社3が管理可能な固有識別子が割り当てられて付与・記録される。そして、決済サービス会社3は、上述のごとく発行され市場に流通している有価データの識別子を、有価データ流通リストに保持して管理することにより、この決済サービス会社3で発行された有価データのうち、現在、市場に流通している全ての有価データを把握している。

【0059】

なお、顧客1がエスクローサービスを利用する旨が手順A16で決済サービス会社3に通知されている場合、決済サービス会社3は、有価データを生成すべく減額処理を行なった預金口座の口座番号も、その有価データの固有識別子とともに記録・保存しておく。

【0060】

同様に、顧客1がエスクローサービスを利用する旨が手順A16で決済サービス会社3に通知されている場合、決済サービス会社3は、有価データを生成するに当たって顧客1の預金口座から減額した現金を一時的に保持しておき、顧客1からの許可がない限り、受取人が有価データを現金化できないようにしておく。このため、決済サービス会社3が、エスクローサービス対象有価データの固有識別子を有価データ流通リストに載せる際に、その有価データについては、顧客1



の許可無しで現金化できないことを示すフラグ（現金化停止フラグ）と、その有価データを生成するために減額した預金口座の口座番号とも、有価データ流通リストに同時に記録しておく。

【0061】

また、本実施形態では、顧客が預金口座に入金した現金から有価データを生成・発行しているが、顧客1と決済サービス会社3とが予め所定の契約を結んでおり、決済サービス会社3が、その顧客1の依頼に応じて行なわれた入金額（支払い額；添付した有価データの相当額）を立て替え、後日、立替額を総計した金額を顧客1に請求し、その金額の現金を顧客1から徴収するようにしてもよい。

【0062】

さらに、本実施形態では、顧客1と決済サービス会社3とは事前に契約しているが（手順A13，A14参照）、このような契約を行わずに、顧客1が決済サービス会社3で現金を直接渡し、その金額に相当する有価データを電子財布Cに投入するようにしてもよい。

【0063】

ところで、図4～図8を参照しながら後述するごとく、有価データは、決済サービス会社3の入金処理によって電子財布C（電子財布本体C0）に連結・接着される。また、前述した通り、正規の受取人以外の利用者は電子財布C（電子財布本体C0）に有価データを添付・追加することしかできず、有価データを単体で電子財布Cから取り出すことができない。この有価データは電子財布本体C0と一緒になければ現金化することができず、しかも、現金化できるのは、電子財布本体C0に登録されている正規の受取人のみである。また、決済サービス会社3で発行され電子財布Cに連結される有価データには、決済サービス会社3による電子署名を添付しておく。このように有価データに電子署名を付けると、有価データの内容（金額等）を改竄できなくなり、有価データの内容の書換えを阻止することができる。

【0064】

〔1-3-4〕電子財布の返送処理

決済サービス会社3で有価データを入金された電子財布Cは、決済サービス会

社3から店舗2へ返送／返却される（矢印A19、A20もしくはA19'、A20'参照；返送ステップ）。その際、電子財布Cは、顧客1を経由して、もしくは、予め登録された顧客1以外の一以上の第三者（例えば承認者4）を経由して、店舗2に返送される。

【0065】

このとき、決済サービス会社3は、電子財布Cを、予め登録された、返送先／経由先（以下、返却先という）としての所定アドレスに電子メール等によって返送／返却する（矢印A19もしくはA19'参照；返送ステップ）。電子財布Cの返却先は、決済サービス会社3側で予め登録されていてもよいし、例えば図2または図3に示すように、電子財布C（電子財布本体C0）自体に予め記録されていてもよい。

【0066】

電子財布Cの返却先を予め決済サービス会社3側に登録しておけば、電子財布Cの返却先を不正に変更することは難しくなり、顧客1は安心して電子財布Cに対する入金を行なえる。また、後述するように、電子財布Cを、顧客1や承認者4を経由させることなく店舗2に直接返送する場合、店舗2に確実に電子財布が返却されるので、電子財布Cが第三者に渡って不正に現金化されたり商取引の邪魔をされたりすることがなくなり、顧客1は安心して店舗2に現金を支払うことができる。

【0067】

また、電子財布Cの返却先を、その電子財布C（電子財布本体C0）自体に予め記録しておけば、利用者〔顧客1、店舗2、第三者（承認者4）〕は、電子財布Cの行き先を自分で確認することができる。また、後述するように、電子財布Cを、顧客1や承認者4を経由させることなく店舗2に直接返送する場合、顧客1は、支払い先が明確になり安心感を得ることができるほか、店舗2は、電子財布Cが必ず自分の所に帰ってくることを確認することができる。

【0068】

顧客1は、図1に矢印A19で示すように、電子財布Cを決済サービス会社3から電子メール等により受け取ると、その電子財布C中の有価データの内容を確

認して電子財布Cに入金された金額を確認する。この後、顧客1は、購入する商品番号等の商品情報や、配達先情報などを追加情報として電子財布本体C0に追加・連結し、さらに電子財布Cの全体に顧客1による電子署名を施してから（図3参照）、その電子財布Cを電子メールやWWW等で店舗2に送信する（矢印A20参照）。今回の決済に当たりエスクローサービスを利用している場合、顧客1は、受け取った電子財布Cのコピーを保存しておく。

## 【0069】

従来のクレジットカードによる支払い方式では、最終的な支払い金額を顧客1が確認することはできなかったため、誤った金額を請求される可能性が残っていた。これは、多くの中小企業では、クレジット決済を完全自動化しているわけではなく、顧客1からの受注内容を改めてC A T端末に社員の手で入力しているからであった。即ち、社員がC A T端末に金額を入力する時に誤りを犯す危険性が残っていた。

## 【0070】

これに対し、本実施形態によれば、上述のごとく電子財布Cを顧客1経由で店舗2に返送することにより、顧客1は、電子財布Cに添付・追加された有価データの内容を最終的に確認して入金金額が正しいかどうかを判断できるとともに、店舗2への代金の支払いをコントロールすることができる。また、入金済み電子財布Cが、決済サービス会社3から顧客の登録アドレスへ返却されるので、電子財布への入金依頼時等に、万一、入金用のパスワードが盗聴されたとしても、そのパスワードを不正に利用して現金を盗み出すことはできない。

## 【0071】

図1に二点鎖線の矢印A19'およびA20'で示すように、電子財布Cを、決済サービス会社3から承認者4経由で店舗2に返送する場合、承認者4は、この電子財布Cを受け取ると（矢印A19'参照）、電子財布C中の有価データの内容を確認して電子財布Cに入金された金額を確認する。その際、購入商品に関する情報が含まれていれば、承認者4は、その情報を参照し、その情報や有価データの金額を考慮して顧客1による今回の商品購入／代金支払いを承認するか否かを判断する。承認しない場合、承認者4は、顧客1や決済サービス会社3にそ

の旨を通知し、今回の電子決済を停止させる。承認する場合、承認者4は、その電子財布Cを電子メールやWWW等で店舗2に送信する（矢印A20'参照）。

## 【0072】

このように、電子財布Cを承認者4経由で店舗2に返送することにより、電子財布Cが店舗2に返送される前に、承認者（第三者）4が、電子財布Cに添付・追加された有価データの内容を最終的に確認して入金金額が正しいかどうかを判断することができる。これは、顧客1と実際の対価の支払い者とが異なる場合などのように購入の承認者（例えば仕事上の上司等の管理者）4が他に存在する場合に有効である。また、支払い者が顧客1とは独立に商取引内容をチェックできるので、例えば顧客1に成りすまして行なわれた商取引に伴う、予期せぬ支払いの発生を監視し、その支払いの実行を確実に阻止することができる。

## 【0073】

なお、電子財布Cを決済サービス会社3から複数の宛先に送信してもよい。つまり、電子財布Cを、複数の宛先を経由させてから店舗2へ送信してもよい。これにより、電子財布Cを受信した人は、有価データの流れを確認することができる。このとき、電子財布Cが複数人に配信されても、電子財布Cに添付された有価データを現金化できるのは、その電子財布本体C0に登録された受取人認証情報によって認証される正規の受取人のみである。従って、第三者は、有価データの内容等を確認することができるだけであり、電子財布Cを受け取ったからといって、有価データを勝手に現金化するなどの不正行為を行なうことはできない。

## 【0074】

また、図1に示す例では、決済サービス会社3は、電子財布Cを顧客1経由もしくは承認者4経由で店舗2に返却しているが、顧客1や承認者4などを経由させることなく、店舗2へ直接送信してもよい。この場合、顧客1が、決済サービス会社3から受け取った電子財布Cを店舗2に送信する必要が無くなるので、顧客1にとっては購入手順が簡略化される。また、決済サービス会社3が不正を働かない限り、顧客1の指定した支払額が店舗2に対して支払われるので、顧客1は安心して商取引を行なうことができる。

## 【0075】

## 〔 1 - 3 - 5 〕 電子財布に対する電子署名付与手法／情報追加手法

電子財布Cの返却先を、電子財布C（電子財布本体C0）に記録する場合、その返却先情報を、図2に示すように電子財布本体C0内に記録してもよいし、図3に示すように電子財布本体C0に追加情報として添付・追加してもよい。ここで、返却先を電子財布C（電子財布本体C0）に記録することに関連して、電子財布本体C0に対する電子署名付与手法／情報追加手法についても併せて説明する。

## 【 0 0 7 6 】

図2に示す第1例では、電子財布Cの返却先が、外部から誰でも確認可能に電子財布本体C0に予め記録されている。決済サービス会社3が電子財布本体C0を発行する時点で電子財布Cの返却先が決まっている場合、例えば電子財布Cを決済サービス会社3から店舗2へ直接返送するような場合、決済サービス会社3が電子財布本体C0を発行する際に、その返送先の情報を発行者情報や所有者認証情報とともに電子財布本体C0に記録することができる。そして、図2に示すように、これらの情報を記録された電子財布本体C0に対して、発行者（決済サービス会社3）の電子署名が付与される。このように電子財布本体C0に電子署名を付与することにより、悪意のある第三者等が、電子財布本体Cに記録されている各種情報を改竄することができなくなり、安全性が高まる。

## 【 0 0 7 7 】

図3に示す第2例では、発行者の電子署名付き電子財布本体C0の発行後、顧客1等の利用者が電子財布本体C0に上記返却先等の各種情報を追加情報として添付・追加している。このとき、追加情報も、その内容を外部から誰でも確認可能に電子財布本体C0に添付される。電子財布Cの返却先は、例えば、入金依頼時に決済サービス会社3へ送付すべき電子財布本体C0に、顧客1によって添付・追加される。また、顧客1や承認者4が、決済サービス会社3からの電子財布Cを店舗2へ送付する際には、店舗2に通知すべき各種情報（商品情報や配送先情報など）を追加情報として電子財布本体C0に添付・追加する。

## 【 0 0 7 8 】

顧客1が電子財布Cの返送先（顧客1もしくは承認者4）を追加情報として電

電子財布本体C 0に添付した場合、図3に示すように、電子財布本体C 0と追加情報とに対して、入金者（ここでは顧客1）の電子署名を付与する。また、顧客1や承認者4が店舗2への通知情報を追加情報として電子財布本体C 0に添付した場合、電子財布本体C 0と追加情報とに対して、顧客1もしくは承認者4の電子署名を付与する。これにより、悪意のある第三者等によって電子財布本体Cに添付された追加情報が改竄されるのが確実に抑止され、安全性が高められるとともに、追加情報を電子財布本体C 0から分離することができなくなる。

#### 【0079】

なお、電子情報本体C 0には、利用者（顧客1、店舗2、決済サービス会社3、承認者4）によって任意のデータ（追加情報）を添付して保存することができる。そのデータとしては、日付、時刻、顧客1の名前、顧客1の住所、顧客1の電話番号、顧客1の電子メールアドレス、対価の支払い理由、対価の金額（入金金額、支払い金額）、商取引で取り扱われる商品の発送先、顧客1所有の電子財布本体（有価データ搬送用電子情報本体；図9の符号K 0参照）等を添付することができる。顧客1所有の電子財布本体K 0を電子財布本体C 0添付する例については、第2実施形態において説明する。

#### 【0080】

このように電子財布Cに顧客1や承認者4が店舗2へ伝えたい事項などを記録できる領域を設けて、電子情報本体に任意のデータを添付できるようにすることにより、顧客1が店舗2へ発注内容などを別便で送付する必要がなくなり、利用者（顧客1や店舗2）の利便性が高まるほか、電子財布Cの入金内容と発注内容との対応関係が明確になり店舗2における管理が楽になる。

#### 【0081】

##### 〔1-3-6〕商品等の発送処理

供給者（店舗）2は、顧客1（もしくは承認者4、決済サービス会社3）から電子財布Cを受け取ると（矢印A 2 0、A 2 0'参照）、その電子財布本体C 0に添付されている有価データの内容（入金金額）や購入商品情報を確認する。このとき、供給者2は、電子署名（電子財布Cの作成者、有価データの作成者、商品情報の作成者の3つ）を用いて、電子財布C内のデータが改竄されていないこ

とを確認する。入金金額が正しく且つデータが改竄されていなければ、供給者2は、電子財布Cに添付された配達先情報を参照し、その配達先（ここでは顧客1宛）に指定の商品等を発送する（矢印A21参照）。

#### 【0082】

本実施形態では、供給者2は、顧客1から有価データ付きの電子財布Cを直接受け取るので、従来のインターネットバンキングによる振込みのごとく供給者2が銀行等からの振込み通知を待つ必要がなくなり、また、電子財布Cに添付された有価データの内容や各種情報を外部から誰でも確認することができるので、供給者2は、即座に入金金額を確認することができる。従って、商品発送までの時間を大幅に短縮することができる。

#### 【0083】

顧客1は、商品等の受け取り後、内容物を確認する。そして、顧客1がエスクローサービスを利用している場合は、顧客1は、商品等を確認した後、保存しておいた電子財布Cのコピーと、電子財布Cに添付された有価データの現金化を許可する旨（有価データの有効／無効通知）とを決済サービス会社3に送信する（矢印A22参照）。そして、決済サービス会社3は、電子財布C中から有価データの識別子を調べ、前記有価データ流通リスト中において有価データの固有識別子とともに記録されている前記現金化停止フラグをリセットし、電子財布Cに添付された有価データを現金化できる状態にする。なお、エスクローサービスの詳細については後述する。

#### 【0084】

##### 〔1-3-7〕有価データの現金化処理

最後に、供給者2は、有価データの入った電子財布Cを決済サービス会社3に持ち込み（矢印A24参照）、この決済サービス会社3で電子財布C内の有価データを現金化してもらう（矢印A25参照）。

決済サービス会社3は、電子財布Cが持ち込まれた場合、有価データの現金化希望者（受取希望者）が、予め登録されている受取人本人（正当な受取人）であるか否かを、電子財布本体C0に記録された認証用情報に基づいて判定する。

#### 【0085】

その際、決済サービス会社3は、現金化希望者から認証対象情報（パスワード、バイオメトリクス情報等）を取得し、認証用情報が受取人認証情報（所有者認証情報）そのものであれば、その受取人認証情報と取得された認証対象情報とを比較し、受取人の認証を行なう。また、認証用情報として電子財布本体C0固有の識別子が用いられている場合には、決済サービス会社3は、その識別子に対応付けてデータベースに登録されている受取人認証情報を読み出してから、読み出された受取人認証情報と取得された認証対象情報とを比較し、受取人の認証を行なう。

## 【0086】

さらに、決済サービス会社3は、現金化対象の有価データに付与された固有識別子が、前記有価データ流通リストに存在するか否かを確認する。もし存在しなければ、その固有識別子をもつ有価データは既に現金化されていることになるので、今回の現金化を行わず、現金化希望者等に対しエラー通知を行なう。

## 【0087】

そして、現金化希望者が正当な受取人であることが認証され、且つ、固有識別子が前記有価データ流通リストに存在していることが確認された場合に限り、決済サービス会社3によって、その有価データの所有権がその現金化希望者に移転される（矢印A25参照；所有権移転ステップ）。つまり、実際には、決済サービス会社3は、その有価データを現金化し、現金を現金化希望者に渡し、前記有価データ流通リストから該当の固有識別子を削除する。

## 【0088】

このとき、決済サービス会社3は、有価データを現金化して得られた現金を、所定の口座に振り込んでもよいし、有価データの受取人本人であると認証された前記現金化希望者に直接手渡してもよい。所定の口座に現金を振り込む場合、現金化希望者は、決済サービス会社3（銀行窓口等）まで出向く必要がなくなる。従って、WWWなどを使用してオンラインで有価データの現金化を行なえるようになり利便性が向上する。現金を現金化希望者に直接手渡す場合、電子財布Cの利用者は、前もって銀行口座等を開設する手間がかからず便利である。

## 【0089】



## 〔 1 - 3 - 8 〕 エスクローサービス

ここで、本実施形態におけるエスクローサービスについて、より詳細に説明する。なお、エスクローサービスとは、互いに信用の置けない二者間（本実施形態では、顧客 1 と供給者 2 との間）で商取引を行なう際、信用の置ける第三者（本実施形態では、決済サービス会社 3）が一時的に現金を預かることで安全な商取引を保証するサービスのことである。

## 【 0 0 9 0 】

前述した通り、顧客 1 がエスクローサービスを用いる場合、決済サービス会社 3 は、顧客 1 の依頼に応じて有価データを発行して電子財布本体 C 0 に添付するとともにその有価データに対応した現金を預金口座から減額した際に、その現金を一時的に保持することにより、その有価データを直ちには現金化できない状態に維持しておく。

## 【 0 0 9 1 】

この後、顧客 1 が、電子財布 C に添付された有価データの現金化を許可する旨を決済サービス会社 3 に通知しなければ、供給者 2（現金化希望者）は、有価データを現金化することができない。もし、顧客 1 が店舗 2 から受け取った商品等が、壊れていたり、所望のものと異なったりしている場合、顧客 1 は、有価データの現金化許可通知を行なわないため、供給者 2 いつまでも現金を手に入れられない。

## 【 0 0 9 2 】

顧客 1 と供給者 2 との話し合いにより、商品等を返品することになった場合、顧客 1 は有価データの無効化を許可する旨を決済サービス会社 3 に通知するとともに（矢印 A 2 2 参照）、供給者 2 は、顧客 1 から受け取った電子財布 C を、供給者 2 の所有者認証情報（指紋データ、パスワード等）とともに、ペンディングされている有価データの発行元である決済サービス会社 3 に送り、その有価データの無効化を承認する旨を決済サービス会社 3 に通知する（矢印 A 2 3 参照）。

## 【 0 0 9 3 】

そして、決済サービス会社 3 は、所有者認証情報に基づいて正当な電子財布所有者（正当な受取人）からの依頼であることを確認し、その後、受け取った電子

財布Cから有価データの識別子を調べ、その識別子が前記有価データ流通リストに存在するか否かを確認する。無効化を承認した供給者2が正当な所有者であり且つ固有識別子が前記有価データ流通リストに存在していることが確認された場合、決済サービス会社3は、一時的に保持されていた現金を顧客1の預金口座に戻してその預金口座の残高を増やす。従って、顧客1が有価データの無効化を依頼するとともに供給者2が有価データの無効化を承認した場合、顧客1が支払った代金が、顧客1の預金口座に戻ってくることになる。決済サービス会社3は、有価データの返金を行なった後、前記有価データ流通リストから有価データの固有識別子を削除する。

## 【 0 0 9 4 】

なお、もし顧客1が有価データの有効化通知を行なわず、供給者2も有価データの無効化承認（返却依頼）を行なわない場合、有価データに相当する代金（現金）は、決済サービス会社3が保持し続けることになる。

また、電子財布C中に所有者認証情報が記録されておらず、且つ、電子財布Cの発行元（第1決済サービス会社；例えばA銀行）と有価データの発行元（第2決済サービス会社；例えばB銀行）とが異なっている場合、第2決済サービス会社は、現金化希望者が電子財布Cの正当な所有者（正当な受取人）であることを検証できない。このような場合は、第2決済サービス会社は、受け取った電子財布Cと所有者認証情報とを第1決済サービス会社へ送信し、正当な所有者からの依頼であることを確認してもらう。なお、2以上の異なる決済サービス会社によって電子財布Cを取り扱う場合については図4～図8を参照しながら後述する。

## 【 0 0 9 5 】

一般的なエスクローサービスは、前述した通り上記手順（b1）～（b6）で行なわれる。これに対し、本実施形態にエスクローサービスを適用した時の処理手順の一例をまとめて記述すると、以下の（B1）～（B7）の通りである。

（B1）顧客1が供給者2から電子財布本体C0をダウンロードする（矢印A15参照）。

## 【 0 0 9 6 】

（B2）顧客1は、電子財布本体C0に発注内容を記述した資料を添付／記入

し、決済サービス会社3、顧客ID、顧客認証情報、入金金額とともに送る（矢印A16参照）。なお、発注内容は、この手順（B2）ではなく、後述する手順（B4）で電子財布本体C0に添付／記入するようにしてもよい。手順（B4）で発注内容を添付すれば、その発注内容が決済サービス会社3に知られるのを防止することができる。

【0097】

（B3）決済サービス会社3は、顧客1の本人認証を行ない、契約口座から指定金額だけ現金を引き出し、一時的に預かる。また、指定された金額に相当する有価データを生成し、電子財布Cに入金する。ただし、この有価データは、この時点では現金化できない状態になっている。決済サービス会社3は、電子財布Cを、顧客1に返却・送信する（矢印A19参照）。

【0098】

（B4）顧客1は、決済サービス会社3から受け取った電子財布Cの中身（入金金額等）を確認し、供給者2に送信する（矢印A20参照）。このとき、顧客1は、電子財布Cのコピーを作成して保存しておく。

（B5）供給者2は、電子財布Cに記録された発注内容と入金金額とを確認してから、商品等を顧客1に発送する（矢印A21参照）。

【0099】

（B6）顧客1は、到着した発注品が所望品であることを確認した後、対応する有価データの現金化を許可する旨と、電子財布Cのコピーと、顧客IDと、顧客認証情報とを決済サービス会社3に送信する（矢印A22参照）。この後、決済サービス会社3は、顧客1の本人認証を行ってから、電子財布C内の有価データを現金化できる状態にする。

【0100】

（B7）供給者2と顧客1との間でトラブルが発生した場合には、そのトラブルが解決するまで、前記有価データは、決済サービス会社3において、現金化できない状態に維持される。そして、顧客1が商品等を供給者2に返品することになった場合、電子財布C内の有価データを無効化する旨と、電子財布Cのコピーと、顧客IDと、顧客認証情報とを決済サービス会社3に送信する（矢印A22

参照)。供給者 2 は、顧客 1 から受け取った電子財布 C を、供給者 2 の所有者認証情報（指紋データ、パスワード等）とともに、ペンディングされている有価データの発行元である決済サービス会社 3 に送り、その有価データの無効化を承認する旨を決済サービス会社 3 に通知する（矢印 A 2 3 参照）。そして、決済サービス会社 3 は、所有者認証情報に基づいて正当な電子財布所有者（正当な受取人）からの依頼であることを確認し、その後、受け取った電子財布 C から有価データの識別子を調べ、その識別子が前記有価データ流通リストに存在するか否かを確認する。無効化を承認した供給者 2 が正当な所有者であり且つ固有識別子が前記有価データ流通リストに存在していることが確認された場合、決済サービス会社 3 は、顧客 1 の本人認証を行ってから、電子財布 C 内の有価データを無効化し、一時的に保持されていた現金を顧客 1 の預金口座に戻してその預金口座の残高を増やす。

## 【 0 1 0 1 】

ここで説明した例では、有価データの有効化／無効化の指示に際して、顧客 1 から決済サービス会社 3 に対し、電子財布 C のコピーを直接送っているが、各有価データに管理識別子を割り当て、この管理識別子を用いて顧客 1 と決済サービス会社 3 との間で特定の有価データを指示し合ってもよい。

## 【 0 1 0 2 】

## 〔 1 - 3 - 9 〕 電子財布本体に対する有価データ連結手法

本実施形態においては、有価データは、以下に説明するごとく決済サービス会社 3 の入金処理によって電子財布 C（電子財布本体 C 0）に連結・接着される。そして、正規の受取人以外の利用者は電子財布 C（電子財布本体 C 0）に有価データを添付・追加することしかできず、有価データを単体で電子財布 C から取り出すことができない。この有価データは電子財布本体 C 0 と一緒になければ現金化することができず、しかも、現金化できるのは、電子財布本体 C 0 に登録されている正規の受取人のみである。つまり、本実施形態の電子財布 C（電子財布本体 C 0）は、有価データを追加する機能のみを持ち、有価データを取り出す機能を持たないように構成されている。

## 【 0 1 0 3 】

また、本実施形態では、決済サービス会社3が有価データを発行すると、その有価データに、決済サービス会社3が管理可能な固有識別子が割り当てられ、市場に流通している有価データの識別子が、有価データ流通リストによって管理される。

上述のような電子財布Cの機能と有価データ流通リストによる管理とにより、セキュリティ維持（複製防止や二重使用防止）のために複雑なシステムを構築する必要がなくなる。以下、この点について詳しく説明する。

【0104】

従来のオンライン決済に用いられる方式、例えば、電子マネー／電子小切手による決済方式や、クレジットカードによる決済方式では、偽造対策に多大なコストをかけなければならなかった。特に、電子マネーや電子小切手は、デジタルデータであるため、簡単に複製されてしまう。従来より、このような偽造を阻止するために様々な工夫がされている。

【0105】

（C1）電子マネーの偽造対策

（C1-1）電子マネーをICカードに記録することにより、磁気カードのように記録データを簡単に複製できないようにする。

（C1-2）専用のリーダ／ライタ（読み書き装置）でないと、電子マネーにおけるデータの書き換えを行なえないようにする。

（C1-3）人対人の対面での商取引を行なう時のみに電子マネーを用い、オンライン上での決済に際しては、電子マネーを使わないようにする。即ち、電子マネー（有価データそのもの）をインターネットには流さない。

（C1-4）ICカード中に記録される電子マネーデータには、暗号化処理を施す。

【0106】

（C2）電子小切手の偽造対策

（C2-1）通常、電子小切手帳が、電子小切手サービス会社によって利用者（受給者、顧客1）に発行され、利用者は、その電子小切手帳から、随時、電子小切手を発行していく。このとき、電子小切手には唯一の識別子（通し番号、

管理番号) が割り当てられている。電子小切手サービス会社は、電子小切手の二重現金化を阻止するため、過去に現金化された電子小切手通し番号を全て保持している。この場合、前記項目〔c 2 - 3〕でも説明した通り、電子小切手サービス会社は、現金化済みの電子小切手の識別子を半永久的に保存し続けなければならない、データベースに保存されるべき識別子のデータ量は膨大なものとなる。従って、極めて大容量の記憶装置が必要であり、システムの構築に莫大なコストを要することになる。

#### 【 0 1 0 7 】

(C 2 - 2) 電子小切手は、誰でも現金化できるため、万一盗難に遭うと、その電子小切手を盗んだ者によって簡単に現金化されてしまう。例えばインターネット上での盗聴によって電子小切手が現金化する前に盗まれた場合、この現金化を阻止する方法はない。また、電子小切手の発行者が、故意に複製し、その複製物を複数の取引相手に渡すことも考えられる。この場合、電子小切手を受け取った供給者 2 などは、その電子小切手を現金化した後に初めて商品等の発送を行なうことになり、発送処理の即時性に欠ける。つまり、電子小切手そのものは有価データとはなり得ず、電子小切手の識別子等を一々確認するか、もしくは、簡単に複製できないような仕組み（例えば電子小切手配送専用プロトコルなど）を開発・作成するかなければならない。

#### 【 0 1 0 8 】

##### (C 3) クレジットカードの偽造対策

クレジットカード決済では、基本的にクレジットカード番号や有効期限を入力するだけなので、成りすましによる不正行為は極めて容易になされてしまう。そのため、クレジットカード会社は、保険を掛けてクレジットカード不正使用にそなえている。

#### 【 0 1 0 9 】

電子マネー、電子小切手、クレジット決済では、偽造対策として、上述のような仕組みを作る必要がある。

本実施形態では、上述した通り、電子財布 C に有価データを追記する機能しか持たせないようにするとともに、有価データの発行元（決済サービス会社 3）に

において、市場に流通している有価データの識別子を有価データ流通リストによって管理している。

【 0 1 1 0 】

このようにすれば、以下のような理由（D 1）～（D 4）により、基本的に、電子財布Cの複製対策のために特別なシステムを構築する必要が無くなる。逆に、利用者が電子財布Cを複製して自由にバックアップを取ることの可能な環境を提供できるので、利用者の安心感をより高めることが可能になる。

（D 1）後述するごとく電子財布本体Cに対し各有価データが連結・接着されているので、正規の受取人以外の利用者は電子財布Cから個々の有価データを取り出すことができず、個々の有価データに対する複製防止機構が不要である。有価データの移動には、必ず電子財布本体C 0 が伴う。電子マネーや電子小切手は、それ単体で移動が可能となっていた。

【 0 1 1 1 】

（D 2）電子財布C中の有価データは、電子財布Cの所有者認証情報と一致する者（正規の受取人）のみによって現金化されるので、電子財布Cを不正に複製しても第三者が現金を手に入れることができない。これに対し、電子マネーや電子小切手は誰でも現金化できてしまうし、クレジットカードは、第三者によって簡単に不正利用されてしまう。

【 0 1 1 2 】

（D 3）電子財布Cには、有価データを追記することしかできないので、最新の電子財布Cしか意味を持たない。即ち、複製した過去の電子財布Cは、最新の電子財布Cよりも価値（有価データの数）が小さいので、利用価値がなくなる。従って、電子財布Cの所有者が、電子財布Cの複製品を用いて不正を働こうとしても、無意味である。

【 0 1 1 3 】

（D 4）本実施形態では、顧客 1 が供給者 2 に電子財布Cにより代金を支払う際に、その電子財布Cが、必ず決済サービス会社 3 側のシステムを通過することになる。従って、決済サービス会社 3 は、電子財布Cに対して発行・入金した全ての有価データに固有識別子（管理番号）を付与することができる。つまり、決

決済サービス会社 3 は、市場に流通している有価データの管理番号を有価データ流通リストに保持し、現金化された有価データの管理番号を有価データ流通リストすることにより、膨大な量のデータを保存することなく、有価データの二重使用（二重現金化）をチェックして二重使用を防止するシステムを、安価に構築することができる。また、市場を流通している有価データが決済サービス会社 3 側で有価データ流通リストによって常に把握されているため、正規の受取人が電子財布 C のコピーを作成して二重使用を行なおうとしても、偽造有価データを簡単に発見でき、一度、現金化された有価データを、再度、現金化することは不可能である。

## 【 0 1 1 4 】

さて、ここで、図 4 ～ 図 8 を参照しながら、電子財布 C（電子財布本体 C 0）に有価データを連結・接着する手法（追加・保存手法）について具体的に説明する。

電子財布 C に有価データを保存する際、電子財布 C に電子署名を施せば、有価データのみを電子財布 C から取り出すことは不可能になる。つまり、決済サービス会社 3 は、電子財布本体 C 0 に有価データを添付・追加する都度、電子財布本体 C 0 と追加された有価データとを含む部分に対する電子署名を作成して、電子財布 C に添付することにより、第三者は電子財布 C を改竄することができなくなり、つまりは電子財布 C に有価データが接着されることになる。このように電子署名を用いて有価データの連結・接着を行なう手法の具体例を、図 4 ～ 図 6 に示す。

## 【 0 1 1 5 】

図 4 に、電子署名を用いた手法の第 1 例を示す。この第 1 例では、決済サービス会社 3 は、電子財布本体 C 0 と、電子署名によってこの電子財布本体 C 0 に既に連結されている有価データと、追加された有価データとの全てに対する電子署名を作成して、電子財布 C に添付している。

## 【 0 1 1 6 】

つまり、図 4 に示す例では、まず、空の電子財布 C に、A 銀行（第 1 決済サービス会社）が発行した 2 0 0 0 円相当の有価データ（第 1 有価データ）を入金す



る。このとき、電子財布本体C0と第1有価データとを連結し、その全体にA銀行の電子署名（A銀行の持っている秘密鍵を使った電子署名）を添付する。電子署名が付与されるため、電子財布本体C0と第1有価データとを切り離すなどの改竄は不可能になる。つまり、第1有価データだけを電子財布Cから取り出すことは不可能となる。なお、ここでは、電子財布本体C0は、A銀行が発行したものであり、この電子財布本体C0には、発行者情報としてA銀行に関する情報が記録されているものとする。

## 【0117】

さらに、上述のような電子財布Cに、B銀行（第2決済サービス会社）が発行した500円相当の有価データ（第2有価データ）を入金する場合を考える。このとき、A銀行発行の第1有価データが添付された電子財布Cに、さらにB銀行発行の第2有価データを連結する。その後、電子財布本体C0、第1有価データ、A銀行の電子署名および第2有価データの全体に、B銀行の電子署名（B銀行の持っている秘密鍵を使った電子署名）を添付する。このような電子署名を付与することにより、A銀行発行の第1有価データはもちろんのこと、B銀行発行の第2有価データも、電子財布Cから単体で取り出せなくなる。

## 【0118】

次に、図5および図6に、電子署名を用いた手法の第2例を示す。上述した第1例では、有価データを追加する都度、電子財布Cの全体に対する電子署名を付与しているが、第2例では、決済サービス会社3は、電子財布本体C0と追加された有価データとの二つに対する電子署名を作成して、電子財布Cに添付している。

## 【0119】

つまり、図5に示す例では、まず、空の電子財布Cに、A銀行（第1決済サービス会社）が発行した2000円相当の有価データ（第1有価データ）を入金するとき、電子財布本体C0と第1有価データとに対するA銀行の電子署名（A銀行の持っている秘密鍵を使った電子署名）を作成し添付する。これにより、第1有価データだけを電子財布Cから取り出すことは不可能となる。ここでも、電子財布本体C0は、A銀行が発行したものであり、この電子財布本体C0には、発

行者情報としてA銀行に関する情報が記録されているものとする。

【0120】

さらに、上述のような電子財布Cに、B銀行（第2決済サービス会社）が発行した500円相当の有価データ（第2有価データ）を入金する場合、電子財布本体C0と第2有価データとに対するB銀行の電子署名（B銀行の持っている秘密鍵を使った電子署名）を作成し添付する。これにより、A銀行発行の第1有価データもB銀行発行の第2有価データも、電子財布Cから単体では取り出せなくなる。この時点で、電子財布Cは、電子財布本体と、A銀行発行の第1有価データと、A銀行の電子署名と、B銀行発行の第2有価データと、B銀行の電子署名とで構成されることになる。

【0121】

図5では、第1有価データおよび第2有価データを入金した電子財布Cに、さらに、A銀行が発行した10000円相当の有価データ（第3有価データ）を入金している。このとき、上述と同様、電子財布本体C0と第3有価データとに対するA銀行の電子署名を作成し添付する。

【0122】

図5に示す手法では、電子財布C中の有価データ同士は、電子署名によって接着接されていないため、図6に示すように、個々の有価データを切り離すことができる。ただし、個々の有価データを取り出す場合でも、電子署名の対象が電子財布本体C0と各有価データとの二つであるので、有価データを電子財布本体C0から切り離すことはできない。即ち、有価データを取り出すとき、電子財布本体C0を複製しなければならない。従って、有価データのみを単体で取り出して他の電子財布に入金するなどして第三者が現金化することは、依然不可能になっている。

【0123】

さて、図4～図6に示す例では、有価データを追加する度に電子財布本体C0を含めた電子署名を作成し、電子財布Cと有価データとの接着を実現しているが、有価データを特定の公開鍵で暗号化することによっても、電子財布Cと有価データとの接着を実現できる。このとき、暗号化に用いられた公開鍵に対応する秘

密鍵は、決済サービス会社 3 および正規の受取人（本実施形態では電子財布 C の所有者／管理者である供給者 2）のうちの少なくとも一方によって保持・管理される。このように公開鍵を用いて有価データの連結・接着を行なう手法の具体例を、図 7 および図 8 に示す。

#### 【 0 1 2 4 】

図 7 および図 8 に示す例において、電子財布本体 C 0 は、A 銀行（第 1 決済サービス会社）が発行したものであり、この電子財布本体 C 0 には、発行者情報として A 銀行に関する情報が記録されるとともに、所定の公開鍵（暗号化公開鍵）も記録されている。

#### 【 0 1 2 5 】

そして、空の電子財布 C に、B 銀行（第 2 決済サービス会社）が発行した 5 0 0 円相当の有価データ（第 1 有価データ）を入金する際、図 7 に示すように、第 1 有価データを、電子財布本体 C 0 に記録された暗号化公開鍵で暗号化し、暗号化された第 1 有価データを電子財布本体 C 0 に添付する。続けて他の有価データを電子財布 C に入金するときは、その有価データも公開鍵で暗号化して添付すればよい。例えば、図 7 に示した電子財布 C に、A 銀行が発行した 5 0 0 円相当の有価データ（第 2 有価データ）を入金する場合、図 8 に示すように、第 2 有価データを、電子財布本体 C 0 に記録された暗号化公開鍵で暗号化し、暗号化された第 2 有価データを電子財布本体 C 0 に添付している。なお、図 7 および図 8 に示す有価データには、それぞれ発行元の電子署名が付与されている。

#### 【 0 1 2 6 】

公開鍵に対応する秘密鍵は、決済サービス会社 3 もしくは供給者 2 によって保持・管理される。上述のごとく暗号化された有価データを正しく復号化するためには、当然、秘密鍵が必要になるので、有価データを実体化できるのは、決済サービス会社 3 もしくは供給者 2 に限定されることになる。このとき、有価データを復号化する秘密鍵を決済サービス会社 3 のみが保持しておく、電子財布 C に保存されている有価データを実体化して取り出せるのは、決済サービス会社 3 のみとなる。従って、第三者が電子財布 C から有価データのみを取り出すことができなくなる。

## 【 0 1 2 7 】

また、上述のように公開鍵を電子財布本体C0に記録しておけば、電子財布Cへの入金処理を行なう決済サービス会社3は、即座に公開鍵を入手して有価データを暗号化することができる。その際、さらに、電子財布Cに電子署名を施しておけば、公開鍵も改竄できなくなるので、より安全性を高めることができる。

さらに、有価データを復号化する秘密鍵をメモリカードなどの可搬型記録媒体に記録しておき、その可搬型記録媒体を、正規の受取人である供給者2が保持・管理するようにしてもよい。これにより、有価データの読み出し即ち現金化は、秘密鍵を記録した可搬型記録媒体の所持者でしかできなくなる。

## 【 0 1 2 8 】

また、図7及び図8に示す例では、暗号化公開鍵を電子財布本体C0に記録しているが、電子財布Cに有価データを保存する都度、暗号化公開鍵を、公的認証機関や決済サービス側など信用できる機関（信用機関）から随時取得するようにしてもよい。この場合、電子財布Cに識別子を割り当てて置き、その識別子を用いてその電子財布Cの公開鍵を取得する。このようにすることで、第三者による公開鍵の書き換えが難しくなり、安全性がより高まる。

## 【 0 1 2 9 】

なお、図4～図8に示す例では、顧客1の依頼に応じて、一つの電子財布本体C0に、2以上の異なる決済サービス会社（A銀行、B銀行）によって2以上の有価データが発行されて添付されている。つまり、本実施形態の電子財布Cには異なる決済サービス会社が発行する複数の有価データを保存することができるようになっている。

## 【 0 1 3 0 】

これにより、顧客1と供給者2との間の商取引に柔軟性が増し、顧客1および供給者2の双方とも便利になる。つまり、顧客1と供給者2とは同じ決済サービス提供者3を利用する必要がなくなる。このように一つの電子情報本体C0に複数の金融機関が発行した電子小切手等の有価データを持たせると、電子情報本体C0の使い勝手は通常の電子マネーと同じになり、通常の電子マネーと変わらない利便性（匿名性、誰でも使える環境）を利用者に提供することが

できる。

【 0 1 3 1 】

また、決済サービス会社 3 において有価データを現金化する際に、電子財布 C に、異なる決済サービス会社によって発行された 2 以上の有価データが含まれている場合、決済サービス会社 3 は、各有価データの発行元である決済サービス会社から、各有価データに対応する現金を集金する。このように、電子財布 C の発行元が各決済サービス会社と協調して各有価データを現金化すれば、有価データの受取人（電子財布 C の所有者／管理者等）は、複数の決済サービス会社と交渉する必要が無くても済み、便利である。

【 0 1 3 2 】

〔 1 - 3 - 1 0 〕 第 1 実施形態の変形例

上述した第 1 実施形態では、顧客 1 が決済サービス会社 3 と契約し電子財布 C に対する入金準備を行なう際に、決済サービス会社 3 が、顧客 ID やパスワードなどを発行して顧客 1 に渡していた。このとき、決済サービス会社 3 は、利用者（顧客 1）が支払い可能な額を記録した電子情報（電子小切手帳）を生成し、顧客 ID の代わりに渡してもよい。

【 0 1 3 3 】

電子小切手帳には、常に利用者が支払える限度額（支払可能額情報）が記録されており、随時、確認することができる。この電子小切手帳を用いた電子財布 C への入金および電子決済は、次のような手順（E 1）～（E 9）で行なわれる。

（E 1）顧客 1 が決済サービス会社 3 と契約し預金口座を開いた後、預金口座に入金する。

【 0 1 3 4 】

（E 2）決済サービス会社 3 は、顧客 1 の口座残高から顧客 1 が支払い可能な額（支払可能額情報）と ID とを記録した電子小切手帳を発行して顧客 1 に預ける。また、決済サービス会社 3 において、パスワード、バイオメトリクス情報などの受取人認証情報（顧客の本人認証情報、所有者認証情報）を決定して保存しておく。このとき、受取人認証情報を、電子小切手帳に暗号化して記録してもよい。

【0135】

(E3) 顧客1が供給者2からの購入物を決定する。

(E4) 顧客1は、手元の電子小切手帳を確認し、残高があるかどうかを確認する。

(E5) 顧客1は、供給者2から電子財布本体C0をダウンロードし、電子財布本体C0に購入物等の情報を添付する。

【0136】

(E6) 顧客1は、電子小切手帳と電子財布Cとを、本人認証情報や入金金額とともに、決済サービス会社3に送信し、商取引に必要な対価に対応する価値を有する有価データを電子財布本体C0に添付するように決済サービス会社3に依頼する。

(E7) 決済サービス会社3は、顧客1の本人認証を行ない、指定された入金金額に相当する有価データを生成し、電子財布Cに入れる。また、以後、顧客1が支払うことの可能な残高（電子小切手帳の支払可能額情報から有価データの価値に応じた額を減額した支払可能額情報）を記録した新たな電子小切手帳を作成する。そして、電子財布Cと新たに作成された電子小切手帳とを顧客1に送信する。

【0137】

(E8) 顧客1は、受け取った電子財布Cと電子小切手帳とを確認する。電子財布Cは、供給者2に送る。以後、古い電子小切手帳は破棄し、送られてきた新たな電子小切手帳を用いるようにする。

(E9) 供給者2は電子財布Cの中身を確認し、所望の商品を発送する。

【0138】

このとき、電子小切手帳には、常に顧客1が支払える限度額（支払可能額情報）が記録されており、顧客1は、随時、その限度額を確認することができる。つまり、顧客1は、常に手元で素早く残高を確認することができる。従って、顧客1は、自分の預金口座の残高を、わざわざ決済サービス会社3にアクセスして確認したり、残高を自分で覚えておいたりする必要がなくなり、顧客1の利便性をより高めることができる。また、ここで説明した例では、顧客1が予め預金口座

に入金しているが、一般的なクレジットカードによる信用取引を行ない、顧客受給側の支払能力から電子小切手帳に記録する残高を決定しても良い。

【0139】

なお、電子財布本体C0に添付される有価データは、電子通貨、電子証券、電子チケットおよび電子許可証のうちの少なくとも一つの機能を有するものであればよく、一つの電子財布本体C0に、2以上の異なる種類の有価データを添付してもよい。このように、一つの電子財布Cに、通貨相当の有価データや、チケット相当の有価データなど、複数の種類の有価データを記録保持できるようにしておけば、顧客1（または電子財布所有者）は複数の電子財布を使い分ける必要がなくなり、顧客1（または電子財布所有者）の利便性をより高めることができるほか、その所有者を明確にすることができる。また、店舗2が電子チケットや電子許可証を商品等として顧客1に発送する場合に、顧客1所有の電子財布K（図9参照）を利用してもよく、その具体例については第2実施形態で後述する。

【0140】

#### 〔1-4〕第1実施形態の効果

上述したように、第1実施形態の電子決済方法では、決済サービス会社3は、入金操作は誰でもできるが現金化（出金）は所有者しかできない電子財布Cを供給者（店舗）2に発行する。そして、本発明の電子決済方法における最大の特徴は、顧客1、店舗2および決済サービス会社3（必要に応じて承認者4も）の相互間で、上述のような電子財布Cをやり取りして決済を行なう点である。

【0141】

以下に、このような第1実施形態の電子決済方法によって得られる作用・効果をまとめて記載する。

〔1-4-1〕顧客1、供給者2、決済サービス会社3の間で、店舗2所有の電子財布C（電子財布本体C0）をやり取りすることにより、顧客1は、決済サービス会社3を介して供給者2に商取引に必要な対価を電子的に支払うことができる。このとき、顧客1は、直接、供給者2への代金の支払いをコントロールすることができるので、顧客1が安心して決済を行なえ、インターネット等を利用した電子商取引を活発化させ売上を大幅に向上させることができる。

【0142】

〔1-4-2〕 決済サービス会社3が顧客1の依頼に応じて有価データを発行することにより、決済サービス会社3が、市場に流通している有価データを全て把握することができ、システムのセキュリティを維持する仕組み（二重使用防止システム）を簡素化できそのシステムを安価に構築することができる。

【0143】

〔1-4-3〕 決済サービス会社3が顧客1の依頼に応じて有価データを電子財布本体C0に添付するので、供給者2のシステムを一切介在させることなく決済が行なわれる。また、供給者2が決済サービス会社3に取引内容を通知する必要がなくなる。従って、供給者2（店舗側の社員等）が操作ミスにより請求金額を誤ったり、供給者2の不正行為（詐欺等）により顧客1が現金を奪われたりすることを一切排除できる。また、現金移動時にクレジットカード番号、パスワードなどの秘密情報が供給者2に漏れることもなくなるとともに、その秘密情報がインターネット等のネットワーク上で盗聴・盗難に遭うこともなくなる。

【0144】

〔1-4-4〕 供給者2が決済サービス会社3に取引内容を通知する必要がなく、電子財布本体C0に添付された有価データに顧客1の情報が含まれておらず、さらに、電子小切手のごとく電子署名に顧客1の署名を使用しないので、顧客1のプライバシーが確実に保護される。

【0145】

〔1-4-5〕 供給者2は、決済サービス会社3から返送されてきた、有価データを添付された電子財布Cを受け取るので、即座に入金金額を確認して、顧客1が入力ミスや悪意のある操作などを行っていないかどうかを直ちに判断することができ、商品等の発送までの時間を短縮することができる。また、入金通知処理も自動化することができるほか、顧客1との取引の度にクレジット会社等と通信する必要がなくなるため、自動化システム構築のコストを低く抑えることができる。

【0146】

〔1-4-6〕 電子財布本体C0に添付された有価データの現金化（所有権



の移転)は、その電子財布本体C0に予め登録された受取人本人(本実施形態では電子財布Cの所有者/管理者である供給者2)しか行なえないので、万一、有価データを含む電子財布Cが盗難されたり複製されたりして、受取人本人以外が有価データを現金化しようとしても、現金化を行なうことができない。従って、不正な現金化を確実に阻止することができる。

## 【0147】

〔1-4-7〕電子財布本体C0に、この電子財布本体C0の発行元(決済サービス会社3)に関する発行元情報を外部から確認可能に記録しておくことにより、電子財布本体C0の発行元を誰でも確認することができる。これにより、その電子財布本体C0に添付された有価データを必ず現金化できることが保証され、利用者(供給者2)に安心感を与えることができる。

## 【0148】

〔1-4-8〕電子財布本体C0に有価データを外部から確認可能に添付することにより、有価データを添付された電子財布本体C0を決済サービス会社3から供給者2へ返送する際に、その電子財布Cを受け取った者〔顧客1や供給者2のほか第三者(承認者4)〕は誰でも有価データの内容(入金金額)を確認することができる。

## 【0149】

〔1-4-9〕有価データを添付された電子財布本体C0を、決済サービス会社3から顧客1経由で供給者2へ返送することにより、電子財布Cが供給者2に返送される前に、顧客1が、支払い金額を最終的に確認し、入金金額が正しいかどうかを判断することができる。このとき、供給者2は、顧客1から直接、有価データ付きの電子財布Cを受け取るので、即座に入金金額を確認することができ、商品等の発送までの時間を大幅に短縮することができる。

## 【0150】

〔1-4-10〕有価データを添付された電子財布本体C0を、決済サービス会社3から、予め登録された顧客1以外の一以上の第三者、例えば承認者4経由で供給者2へ返送することにより、電子財布Cが供給者2に返送される前に、承認者4が、支払い金額を最終的に確認し、入金金額が正しいかどうかを判断す

ることができる。これは、顧客1と実際の対価の支払い者とが異なる場合などのように購入の承認者4が他に存在する場合に有効である。また、支払い者が受給者（顧客）1とは独立に商取引内容をチェックできるので、例えば受給者1に成りすまして行なわれた商取引に伴う、予期せぬ支払いの発生を監視し、その支払いの実行を確実に阻止することができる。

## 【0151】

従来、クレジットカードによる支払いでは、クレジットカード番号等を知った者が勝手に商品などを購入できてしまうため、ユーザはクレジットカード番号等を他人に教えないようにしているが、万一、クレジットカード番号等を知られてしまうと悪用される可能性がある。これに対し、本実施形態で説明したように承認者4が顧客1とは独立に必ず購入内容をチェックすれば、顧客1から決済サービス会社3に送信する顧客IDと顧客認証情報とが、盗聴／盗難等によって他人に知られ、悪用されたとしても、その悪用に伴う予期せぬ支払いを確実に阻止することができる。

## 【0152】

〔1-4-11〕電子財布Cの返送先／経由先を決済サービス会社3側に予め登録しておき、その電子財布Cを、決済サービス会社3から、予め登録された返送先／経由先へ返送することにより、電子財布Cの返送先／経由先を不正に変更することは難しくなる。従って、顧客1は安心して、電子財布本体C0に対する入金（有価データの添付）を行なえる。また、供給者2に電子財布Cが直接返送される場合、供給者2に確実に電子財布Cが返却されるので、電子財布Cが第三者に渡って不正に現金化されたり商取引の邪魔をされたりすることがなくなり、顧客1は安心して供給者2に現金を支払うことができる。

## 【0153】

〔1-4-12〕電子財布Cの返送先／経由先をその電子財布C（電子財布本体C0）に予め記録しておき、その電子財布Cを、決済サービス会社3から、予め記録された返送先／経由先へ返送することにより、利用者（顧客1，供給者2，承認者4）は、電子財布4の行き先を自分で確認することができる。また、供給者2に電子財布Cが直接返送される場合、顧客1は、支払い先が明確になり

安心感を得ることができるほか、供給者 2 は、電子財布 C が必ず自分の所に帰ってくるかどうかを確認することができる。

【 0 1 5 4 】

〔 1 - 4 - 1 3 〕 電子財布本体 C 0 に記録された認証用情報を、有価データの受取希望者の認証時にこの受取希望者から取得された認証対象情報と照合されるべき受取人認証情報（所有者認証情報；例えばバイオメトリクス情報やパスワードそのもの）とした場合、受取人（電子財布 C の所有者である供給者 2）と電子財布本体 C 0 との確実な対応関係を築くことができ、受取人本人のみが有価データを現金化することができる。このとき、電子財布本体 C 0 には、図 2 ～ 図 8 に示すように、発行者情報、返却先、暗号化公開鍵のほかに認証用情報（受取人認証情報そのもの）が記録されるだけなので、電子財布 C の匿名性が維持される。また、電子財布本体 C 0 中に受取人認証情報を記録するため、受取人認証情報の管理をするためのシステムが不要である。

【 0 1 5 5 】

〔 1 - 4 - 1 4 〕 電子財布本体 C 0 の固有識別子を認証用情報として電子財布本体 C 0 に予め記録するとともに、有価データの受取希望者の認証時にこの受取希望者から取得された認証対象情報と照合されるべき受取人認証情報（バイオメトリクス情報やパスワードそのもの）を、上記固有識別子に対応付けて、決済サービス会社 3 が保持しておくことにより、受取人本人のみが有価データを現金化することができる。このとき、受取人認証情報は決済サービス会社 3 側で保持され、電子財布本体 C 0 には固有識別子が記録されるだけなので、受取人認証情報の書換による不正な現金化を確実に阻止することができる。また、この場合も、電子財布本体 C 0 には、図 2 ～ 図 8 に示すように、発行者情報、返却先、暗号化公開鍵のほかに認証用情報（電子財布本体 C 0 の固有識別子）が記録されるだけなので、電子財布 C の匿名性が維持される。

【 0 1 5 6 】

〔 1 - 4 - 1 5 〕 上記固有識別子と受取人認証情報（バイオメトリクス情報やパスワードそのもの）とを対応付けたデータを、決済サービス会社 3 で保持する代わりに、可搬型記録媒体に記録しておくことにより、その可搬型記録媒体を

電子財布本体C0の受取人が所持・管理することができ、決済サービス会社3側での受取人認証情報の管理が不要となる。また、バイオメトリクス情報を受取人認証情報として用いる場合、その受取人認証情報のプライバシーを自分自身で管理することができる利点もある。

【0157】

〔1-4-16〕 上述した受取人認証情報（所有者認証情報）として文字列を用いることにより、従来広く用いられているパスワード方式による本人認証と同じ方式を採用することができ、本人認証方式が利用者に受け入れられやすい。

一方、上述した受取人認証情報（所有者認証情報）として受取人本人のバイオメトリクス情報を用いることにより、受取人の本人認証が確実に行なえるようになり、安全性が高まる。また、パスワードのように受取人が受取人認証情報を記憶する必要がなく、受取人認証情報の管理を特別に行なう必要がなくなる。

【0158】

〔1-4-17〕 受取人を、電子財布本体C0の所有者、もしくは、供給者2を管理する管理者とし、受取人認証情報として、その所有者もしくは管理者の認証情報を登録することにより、所有者もしくは管理者と電子財布本体C0との確実な対応関係を築くことができ、有価データの現金化は、所有者もしくは管理者以外是有価データを現金化することができなくなる。

【0159】

〔1-4-18〕 顧客1，供給者2および決済サービス会社3の相互間の情報転送を有線通信手段や無線通信手段のうちの少なくとも一方によって行なうことで、即時性が高くなり、快適に電子決済システムを利用することができる。また、顧客1，供給者2および決済サービス会社3の相互間の情報転送を、可搬型記録媒体をやり取りすることによって行なうことで、オフラインでも電子決済を使用でき、通信環境を整える必要がなくなる。

【0160】

〔1-4-19〕 決済サービス会社3が、顧客1や予め登録された第三者（承認者4）を含む確認先に対し、有価データ添付の実行確認を行なうことにより、不正な現金移動が実行されようとしている場合にその事実が事前に判明し、不

正な現金移動を未然に防止することができるので、安全性をより高めることができる。その際、確認先を決済サービス会社3側に予め登録しておけば、不正な現金移動を発覚させないよう犯罪者等が確認先を書き換えることが困難になる。また、確認先を電子財布C（電子財布本体C0）に予め記録しておけば、その電子財布C（電子財布本体C0）を使用する度に現金移動の確認先を柔軟に変更することができる。

## 【0161】

〔1-4-20〕 決済サービス会社3側における顧客1の預金口座に現金を予め入金しておき、決済サービス会社3が、電子財布本体C0に添付した有価データに対応する金額をその預金口座から減額することにより、決済サービス会社3は、顧客1から予め預かっておいた現金を用いて、電子財布本体C0に対する入金処理を行なうことができるので、顧客1からの集金の手間が省けるとともに、顧客1から入金金額に対応する現金を回収できなくなるというリスクも無くなる。

## 【0162】

〔1-4-21〕 顧客1の預金口座から減額した現金を決済サービス会社3が一時的に保持しておき、決済サービス会社3は、顧客1からの許可を受けて有価データの現金化を行なう一方、顧客1が許可しない場合には、一時的に保持されていた現金を顧客1の預金口座に戻すようにすることで、決済サービス会社3は、顧客1と供給者2との間の商取引に対し、エスクローサービス（第三者仲介）を提供することができる。

## 【0163】

〔1-4-22〕 顧客1が有価データの無効化を決済サービス会社3に依頼した場合、決済サービス会社3、供給者2から有価データの無効化の承認を得た後、一時的に保持されていた現金を顧客1の預金口座に戻すことにより、決済サービス会社3が預かっていた現金は、顧客1および供給者2の両者からの承認が得られないと顧客1の預金口座には戻らず、供給者の安全性も守られるようになる。

## 【0164】

〔1-4-23〕顧客1は、決済サービス会社3と予め契約しておき、決済サービス会社3が、電子財布本体C0に添付した有価データに対応する金額を立て替え、後日、立て替えた金額を顧客1に請求することで、顧客1は、残金を気にすることなく電子財布本体C0に入金でき、顧客1にとって便利になる。この方法は、従来のクレジットカードサービスと同じ仕組みであるので、既存のクレジットカードサービスシステムをそのまま使用することができる。

## 【0165】

〔1-4-24〕正規の受取人以外の利用者が利用できる電子財布本体C0の機能を、電子財布本体C0に有価データを添付・追加する機能のみに限定することにより、決済サービス会社3が市場に流通している有価データを全て管理可能であること、および、受取人本人以外が有価データを現金化することができないことと相俟って、セキュリティ維持（複製防止、二重使用防止）のためのシステム構築がほとんど不要となる。逆に有価データを含む電子財布Cを複製して自由にバックアップできる環境を利用者に提供することができ、利用者は多大な安心感を得ることができる。また、有価データを添付された電子財布Cについて複製防止技術が不要になるため、その電子財布Cを電子メールに添付するなどして顧客1，供給者2，決済サービス会社3，承認者4の相互間で極めて簡単にやり取りすることができる。

## 【0166】

〔1-4-25〕決済サービス会社3が、電子財布本体C0に有価データを添付・追加する都度、電子財布本体C0と追加された有価データとを含む部分に対する電子署名を作成して、電子財布Cに添付することにより、有価データのみを電子財布Cから不正に取り出すことは不可能で、電子財布本体C0に添付された有価データを第三者が不正に現金化することはできない。

## 【0167】

〔1-4-26〕電子財布本体C0に、その電子財布本体C0の発行者による電子署名を添付したり、顧客1が、追加情報を電子財布本体C0に追加した場合、電子財布本体C0と追加情報とに対する電子署名を作成して電子財布本体C0に添付したりすることにより、第三者が、電子財布本体C0に記録されている

各種情報を改竄することができなくなり、安全性が高まる。

【 0 1 6 8 】

〔 1 - 4 - 2 7 〕 電子財布本体 C 0 に添付される有価データを所定の公開鍵により暗号化し、その公開鍵に対応する秘密鍵を、決済サービス会社 3 および顧客 1 のうちの少なくとも一方が管理することにより、有価データを正しく復号化するには、秘密鍵が必要になるので、有価データを実体化（現金化）できるのは、決済サービス会社 3 もしくは受取人（電子財布本体 C 0 の所有者や管理者等；本実施形態では供給者 2）に限定される。

【 0 1 6 9 】

〔 1 - 4 - 2 8 〕 電子財布本体 C 0 に添付される有価データを所定の公開鍵により暗号化し、受取人（電子財布本体 C 0 の所有者や管理者等；本実施形態では供給者 2）が、その公開鍵に対応する秘密鍵を記録された可搬型記録媒体を保持することにより、有価データの読出し即ち現金化は、秘密鍵を記録した記録媒体の所持者（受取人）しか行なえなくなる。

【 0 1 7 0 】

〔 1 - 4 - 2 9 〕 有価データの暗号化に用いられる公開鍵を電子財布本体 C 0 に記録しておけば、電子財布 C に対する入金処理を行なう決済サービス会社 3 は、即座に公開鍵を入手して有価データを暗号化することができる。その際、電子財布本体 C 0 に電子署名を施しておけば、公開鍵を改竄することができないので、安全性を確保することができる。これに対し、有価データの暗号化に用いられる公開鍵を信用機関から随時取得するようにすれば、第三者による公開鍵の書き換えが難しくなり、安全性が高まる。

【 0 1 7 1 】

〔 1 - 4 - 3 0 〕 図 7 や図 8 に示すように、電子財布本体 C 0 に添付される有価データに、決済サービス会社 3 による電子署名を添付することにより、有価データの発行元である決済サービス会社 3 以外の者による有価データの書換えを阻止することができる。

【 0 1 7 2 】

〔 1 - 4 - 3 1 〕 決済サービス会社 3 が、有価データを現金化した際に現金

を所定の口座に振り込むことにより、受取人本人（電子財布本体C0の所有者／管理者である供給者2）は、銀行窓口まで行くことなく、WEBなどを使用してオンラインで現金化を行なえ便利である。これに対し、決済サービス会社3が、有価データを現金化した際に現金を受取人本人であると認証された受取希望者に手渡すことにより、受取人は、前もって口座を開いておく必要が無く、手間がかからないという利点を得られる。

## 【 0 1 7 3 】

〔 1 - 4 - 3 2 〕 本実施形態の電子決済方法では、電子財布Cに対する入金処理は必ず決済サービス会社3側のシステムで行なわれる。従って、決済サービス会社3は、発行した全ての有価データに決済サービス側が固有識別子（管理番号）を付与することができる。つまり、決済サービス会社3は、市場に流通している有価データの識別子を有価データ流通リストで保持・管理することにより、市場に流通している有価データの内、決済サービス会社3が発行したものを全て把握することができる。このとき、現金化対象の有価データに付与された固有識別子が決済サービス会社3の有価データ流通リストに保持されている場合に、その有価データの所有権を受取希望者に移転する、即ち有価データの現金化を行なう。これにより、二重現金化のチェックを安価なシステムで実現できるほか、偽造有価データの発見も極めて簡単に行なえる。

## 【 0 1 7 4 】

〔 1 - 4 - 3 3 〕 電子財布本体C0に、任意のデータ（例えば日付、時刻、顧客1の名前、顧客1の住所、顧客1の電話番号、顧客1の電子メールアドレス、対価の支払い理由、対価の金額、商取引で取り扱われる商品の発送先、顧客1所有の電子財布本体のうちの少なくとも一つ）を添付することにより、顧客1が供給者2に発注内容などを別便で送付する必要がなくなり利用者（顧客1や供給者2）の利便性が高まるほか、電子財布本体C0内の入金内容と発注内容との対応関係が明確になり供給者2の管理が楽になる。

## 【 0 1 7 5 】

〔 1 - 4 - 3 4 〕 供給者2所有の電子財布本体C0を一般公開し、顧客1が、一般公開された電子財布本体C0を取得できるようにすることで、顧客1が必



要なときに電子財布本体C0を取得して発注処理を行なうことができる。つまり、供給者2が各顧客1と個別に対応をとって電子財布本体C0を顧客1に与える必要が無くなる。

【0176】

〔2〕第2実施形態の説明

図9は本発明の第2実施形態としての電子決済方法を適用されるシステムの構成および同方法の手順を説明するための図、図10は第2実施形態における電子チケット（電子許可証）の利用手法を説明するための図である。

本発明の第2実施形態では、顧客1所有の電子財布（有価データ搬送用電子情報）Kを、携帯電話（情報携帯端末；図10の符号10参照）に記録し、この携帯電話10とともに携帯して用いる。この電子財布Kには、有価データとして、例えば会場入場許可証（電子チケット、電子許可証）や各種割引券が入れられている。

【0177】

この第2実施形態では、図9に示すごとく、顧客1が電子チケットを購入するとき、チケット販売会社（供給者2）への支払いをチケット販売会社所有の電子財布Cを用いて第1実施形態で上述した手順で行ない、チケット販売会社2から顧客1へのチケットの受け渡しは、顧客1所有の電子財布Kを用いて行なう（図9の矢印A32参照）。そして、電子チケット入り電子財布Kが携帯電話10に記録され、電子財布Kの内容を携帯電話10の表示部11（図10参照）に表示することにより、電子財布Kが会場5への入場時の本人証明（所有物認証）のために利用される。

【0178】

以下に、図9および図10を参照しながら、顧客1が電子チケットを供給者であるチケット販売会社2から購入して会場5へ入場するまでの手順について説明する。第2実施形態では、チケット販売会社2所有の電子財布Cと顧客1所有の電子財布Kとの2種類の電子財布をやり取りする。ここで、顧客1の電子財布Kは、第1実施形態で前述した供給者2所有の電子財布Cと同様にして、顧客1に対して発行される。

## 【0179】

まず、チケット販売会社2および顧客1は、それぞれ、自分の所有する電子財布C、Kを、どこかの決済サービス会社によって発行してもらい所有しておく。これらの電子財布C、Kは、第1実施形態と同様にして発行される。ただし、図10に示すように、顧客1の電子財布本体（有価データ搬送用電子情報本体）K0には、発行者情報（発行元情報；ここではA銀行に関する情報）と所有者認証情報（受取人認証情報；ここでは顧客1の認証用情報）と有価データ（電子チケット等）を暗号化するための公開鍵とが記録され、さらに発行元のA銀行（決済サービス会社3）による電子署名が添付されている。また、電子チケット入りの電子財布Kを記録される携帯電話10には、暗号化された有価データを復号化するための復号鍵（暗号化公開鍵に対応する秘密鍵）が予め記録されている。

## 【0180】

顧客1は、チケット販売会社2から、WWW等を通して電子財布本体C0をダウンロードして取得する（図9の矢印A15参照）。そして、顧客1は、顧客ID、顧客認証情報（指紋データ、パスワード等の本人認証情報）および入金金額とともに電子財布本体C0を決済サービス会社3に送信する（図9の矢印A16参照）。決済サービス会社3は、顧客IDおよび顧客認証情報を用いて顧客1の本人認証を行なう。そして、指定された金額に相当する有価データを生成し、電子財布Cに連結（入金）する。その後、入金済み電子財布Cを顧客1に返却する（図9の矢印A18参照）。ここまでの入金手順は、第1実施形態において説明した手順と同様である。

## 【0181】

次に、顧客1は、電子財布Cをチケット販売会社2に送付し（図9の矢印A31参照）、所望のチケットを購入する。このとき、顧客1は、自分の電子財布Kを用いて電子チケットを受け取る（図9の矢印A32参照）。このときの詳細な手順を以下に説明する。

顧客1は、購入したいチケットの情報を作成し、この購入情報と自分の電子財布本体K0とともに、入金済み（有価データ入り）の電子財布Cをチケット販売会社2に送る（図9の矢印A31参照）。

## 【 0 1 8 2 】

チケット販売会社 2 は、受け取った電子財布 C から、有価データと購入情報と電子財布 K とを抽出する。有価データの電子署名を確認し、有価データの有効性を確認する。次に、電子財布本体 K 0 の発行元の電子署名を確認し、信頼の置ける機関・法人の発行した電子財布本体 K 0 であることを確認する。その後、購入情報に従って、チケットに相当する有価データ（電子チケット）を生成する。このときの有価データは、例えば、チケットのイメージ画像やバーコード画像、主催内容などが含まれるデータであればよい。そして、生成された有価データにチケット販売会社 2 の電子署名を添付した後、有価データを電子財布本体 K 0 に記録されている公開鍵で暗号化し、暗号化された有価データを電子財布本体 K 0 に連結する。チケット販売会社 2 は、上述のようにして電子チケットを入れられた電子財布 K を顧客 1 の携帯電話 1 0 宛に電子メール等で返却する（図 9 の矢印 A 3 2 参照）。

## 【 0 1 8 3 】

顧客 1 は、携帯電話 1 0 で、電子チケット入り電子財布 K を受け取ると、その電子財布 K を常に携帯電話 1 0 に保持して携帯する。上述した一連の操作を、全て携帯電話 1 0 のデータ通信によって行なうようにすれば、顧客 1 は、オンライン決済をするためのパーソナルコンピュータ等の端末を所有していなくても、携帯電話 1 0 だけでオンラインショッピングを行なうことができ、便利である。

## 【 0 1 8 4 】

顧客 1 が会場 5 に入場する際には、携帯電話 1 0 に記録されている電子財布 K から、有価データとしての電子チケットを取り出し、携帯電話 1 0 に記録されている秘密鍵で復号化する。復号化された電子チケットが、例えばチケットのイメージ画像であれば、それを携帯電話 1 0 の表示部 1 1 に表示し、顧客 1 は、そのイメージ画像を会場 5 の係員に提示して会場 5 に入場する（図 9 の矢印 A 3 3 参照）。復号化された電子チケットが、例えばバーコードであれば、それを携帯電話 1 0 の表示部 1 1 に表示し、顧客 1 は、そのバーコード画像を会場 5 の係員によってバーコードスキャナで読み取ってもらい入場許可者かどうかの判定を受けてから、会場 5 に入場する。このようにして電子チケットを使用した後、顧客 1

は、電子財布Kを破棄する。

【0185】

ここで、チケット販売会社2は、電子財布Kを利用して電子チケットを顧客1に渡しているが、このように電子財布Kを利用する理由について、以下に説明する。

チケット販売会社2がチケット販売において、最も懸念することは、偽造とダブ行為である。電子チケットのオンライン販売においても同じである。従って、これらの不正行為を阻止する方法を用意しなければならない。電子マネーや電子小切手と同じように、チケットを電子化した電子チケット（有価データ）は、それをそのまま顧客とやり取りすると、簡単に偽造されてしまう。電子チケットを偽造できないように（若しくは、偽造しても無意味なように）、電子チケットを利用できる人（顧客）を限定する仕組みが必要である。即ち、電子チケットと顧客とを関連付け、その顧客以外は電子チケットを利用できないようにする仕組みが求められる。

【0186】

このような仕組みの実現に、顧客1の持っている電子財布Kを利用する。本実施形態で提案する電子財布Kは、第1実施形態においても説明した通り、本来、有価データを保持し、その有価データの現金化は、本人以外行なえないような仕組みを提供するものである。即ち、電子財布Kと顧客1とは密接に関連付けられている。この電子財布Kに電子チケットを連結すれば、結果的に電子チケットと顧客1とは密接に関連付けられ、顧客1以外、その電子チケットを使用できなくすることができる。

【0187】

チケット販売会社2は、顧客1の電子財布Kが信用のおける決済サービス会社が発行したものであるかを、電子財布本体K0の電子署名から検証し、電子財布Kと電子財布Kの所有者とが密接に関連付けられたものかどうかを判断する。電子財布本体K0には、有価データの暗号化用の公開鍵が記録されており、それを復号化する秘密鍵は、携帯電話10に記録されている。即ち、電子財布Kの中身を確認できるのは、携帯電話10を持っている人に限定される。電子財布Kを盗

んだり、複製しても、その携帯電話を持っている人でしか、正しく電子チケットを復号化できない。従って、電子チケットの偽造やダフ行為を阻止することができる。

【0188】

これを実現するには、秘密鍵を複製することができない環境を提供しなければならない。これは、携帯電話10に記録する秘密鍵を特定の人（装置）しか書き込めない領域に記録すれば実現できる。例えば、携帯電話10の製造時に携帯電話10の書換え不可能な領域に予め秘密鍵を書き込んでおき、その公開鍵とともに携帯電話10を発売する。この場合、顧客1が決済サービス会社と契約し、電子財布本体K0を作成するときは、携帯電話10に付属している公開鍵を用いて電子財布Kを作成すればよい。電子財布Kと携帯電話10とは、公開鍵・秘密鍵を通して、密接に関連付けられることになる。

【0189】

また、その他の例として、電子財布Kを発行した決済サービス側が秘密鍵を記録したメモリカードを顧客1に渡し、それを携帯電話10に装着することでしか有価データを復号化できないようにしてもよい。このとき、メモリカードの生成は決済サービス側でしかできない仕組みを用意すれば、電子財布Kの安全性は守られる。

【0190】

このように、本発明の第2実施形態によれば、チケット販売会社2が電子チケットや電子許可証を顧客1所有の電子財布Kに添付して顧客1に送付することにより、確実かつ安全に商品を顧客1に受け渡すことができる。その際、決済サービス会社3からチケット販売会社2へ返送される電子財布Cが顧客1を経由した際に、その電子財布Cに顧客1所有の電子財布本体K0体を添付することで、顧客1は、極めて容易にチケット販売会社2に電子財布本体K0を受け渡すことができる。

【0191】

また、顧客1は、電子チケットや電子許可証を添付された電子財布Kを受け取ると、電子チケットや電子許可証の内容を表示させて係員等に提示することによ

り、電子チケットや電子許可証を利用することができる。特に、電子チケットや電子許可証を添付された電子財布Kを携帯電話10で受け取った場合、その電子チケットや電子許可証の内容を携帯電話10の表示部11に表示させて係員等に示すだけで、極めて容易に電子チケットや電子許可証を利用することができる。

【0192】

〔3〕その他

なお、本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。

【0193】

〔4〕付記

（付記1） 受給者と供給者との間で商取引を行なう際に、該受給者が、該商取引に必要な対価を、決済サービス提供者を介して該供給者に電子的に支払うための電子決済方法であって、

該供給者が、有価データを保持する機能を有するとともに該有価データの受取人を認証するために必要な認証用情報を予め記録された有価データ搬送用電子情報本体を取得して所有するステップと、

該受給者が、該供給者所有の該電子情報本体を取得するステップ（以下、取得ステップという）と、

該受給者が、該決済サービス提供者に対し、該電子情報本体を送信するとともに、前記商取引に必要な対価に対応する価値を有する有価データを該電子情報本体に添付するように依頼するステップ（以下、依頼ステップという）と、

該決済サービス提供者が、該受給者の依頼に応じて、該受給者を認証してから、該有価データを該電子情報本体に添付するステップ（以下、添付ステップという）と、

該電子情報本体と該有価データとからなる有価データ搬送用電子情報が、該決済サービス提供者から該供給者へ返送されるステップ（以下、返送ステップという）と、

該有価データ搬送用電子情報における該有価データの受取希望者が、該電子情報本体に記録された該認証用情報に基づいて、該有価データの受取人本人である

と認証された場合に限り、該決済サービス提供者によって、該有価データの所有権が当該受取希望者に移転されるステップ（以下、所有権移転ステップという）を含むことを特徴とする、電子決済方法。

【 0 1 9 4 】

（付記 2） 該電子情報本体に、該電子情報本体の発行元に関する発行元情報が、その内容を外部から確認可能に予め記録されていることを特徴とする、付記 1 記載の電子決済方法。

（付記 3） 該電子情報本体に、該有価データが、その内容を外部から確認可能に添付されていることを特徴とする、付記 1 または付記 2 に記載の電子決済方法。

【 0 1 9 5 】

（付記 4） 前記返送ステップにおいて、該電子情報が、該受給者経由で該供給者に返送されることを特徴とする、付記 3 記載の電子決済方法。

（付記 5） 前記返送ステップにおいて、該電子情報が、予め登録された該受給者以外の一以上の第三者経由で該供給者に返送されることを特徴とする、付記 3 または付記 4 に記載の電子決済方法。

【 0 1 9 6 】

（付記 6） 該有価データ搬送用電子情報の返送先が、該決済サービス提供者側で予め登録されており、

前記返送ステップにおいて、該電子情報が、該決済サービス提供者から、該決済サービス提供者側で予め登録された返送先へ返送されることを特徴とする、付記 1 ～付記 5 のいずれか一つに記載の電子決済方法。

【 0 1 9 7 】

（付記 7） 該有価データ搬送用電子情報の返送先が、該有価データ搬送用電子情報に予め記録されており、

前記返送ステップにおいて、該電子情報が、該決済サービス提供者から、該電子情報に予め記録された返送先へ返送されることを特徴とする、付記 1 ～付記 5 のいずれか一つに記載の電子決済方法。

【 0 1 9 8 】

(付記 8) 該有価データ搬送用電子情報の返送時の経由先が、該決済サービス提供者側で予め登録されており、

前記返送ステップにおいて、該電子情報が、該決済サービス提供者から、該決済サービス提供者側で予め登録された経由先を経由した上で、該供給者へ返送されることを特徴とする、付記 1 ～付記 5 のいずれか一つに記載の電子決済方法。

【 0 1 9 9 】

(付記 9) 該有価データ搬送用電子情報の返送時の経由先が、該有価データ搬送用電子情報に予め記録されており、

前記返送ステップにおいて、該電子情報が、該決済サービス提供者から、該電子情報に予め記録された経由先を経由した上で、該供給者へ返送されることを特徴とする、付記 1 ～付記 5 のいずれか一つに記載の電子決済方法。

【 0 2 0 0 】

(付記 1 0) 該認証用情報が、前記受取希望者の認証時に前記受取希望者から取得された認証対象情報と照合されるべき受取人認証情報であることを特徴とする、付記 1 ～付記 9 のいずれか一つに記載の電子決済方法。

(付記 1 1) 該電子情報本体が、該決済サービス提供者によって発行されたものであり、

電子情報本体固有の識別子が、該認証用情報として、該電子情報本体に予め記録されるとともに、

前記受取希望者の認証時に前記受取希望者から取得された認証対象情報と照合されるべき受取人認証情報が、該識別子に対応付けられて、該決済サービス提供者によって保持されることを特徴とする、付記 1 ～付記 9 のいずれか一つに記載の電子決済方法。

【 0 2 0 1 】

(付記 1 2) 該電子情報本体が、該決済サービス提供者によって発行されたものであり、

電子情報本体固有の識別子が、該認証用情報として、該電子情報本体に予め記録されるとともに、

前記受取希望者の認証時に前記受取希望者から取得された認証対象情報と照合



されるべき受取人認証情報が、該識別子に対応付けられて、可搬型記録媒体に記録されることを特徴とする、付記 1 ～付記 9 のいずれか一つに記載の電子決済方法。

【 0 2 0 2 】

（付記 1 3） 該受取人認証情報が、文字列であることを特徴とする、付記 1 0 ～付記 1 2 のいずれか一つに記載の電子決済方法。

（付記 1 4） 該受取人認証情報が、前記受取人本人から得られるバイオメトリクス情報であることを特徴とする、付記 1 0 ～付記 1 2 のいずれか一つに記載の電子決済方法。

【 0 2 0 3 】

（付記 1 5） 前記受取人が、該電子情報本体の所有者であることを特徴とする、付記 1 ～付記 1 4 のいずれか一つに記載の電子決済方法。

（付記 1 6） 前記受取人が、該供給者を管理する管理者であることを特徴とする、付記 1 ～付記 1 4 のいずれか一つに記載の電子決済方法。

（付記 1 7） 該受給者、該供給者および該決済サービス提供者の相互間の情報転送が、有線通信手段および無線通信手段のうちの少なくとも一方によって行なわれることを特徴とする、付記 1 ～付記 1 6 のいずれか一つに記載の電子決済方法。

【 0 2 0 4 】

（付記 1 8） 該受給者、該供給者および該決済サービス提供者の相互間の情報転送が、可搬型記録媒体をやり取りすることによって行なわれることを特徴とする、付記 1 ～付記 1 6 のいずれか一つに記載の電子決済方法。

（付記 1 9） 前記添付ステップに先立ち、該決済サービス提供者が、該受給者、もしくは、予め登録された該受給者以外の第三者を含む確認先に対し、前記添付ステップの実行確認を行なうことを特徴とする、付記 1 ～付記 1 8 のいずれか一つに記載の電子決済方法。

【 0 2 0 5 】

（付記 2 0） 該確認先が、該決済サービス提供者側で予め登録されていることを特徴とする、付記 1 9 記載の電子決済方法。

(付記 2 1) 該確認先を、該有価データ搬送用電子情報に記録することを特徴とする、付記 1 9 記載の電子決済方法。

【 0 2 0 6 】

(付記 2 2) 該受給者が、該決済サービス提供者側で口座を設け、該口座に現金を予め入金しておき、

前記添付ステップで有価データを該電子情報本体に添付した場合、該決済サービス提供者が、添付した有価データに対応する金額を該口座から減額することを特徴とする、付記 1 ～付記 2 1 のいずれか一つに記載の電子決済方法。

【 0 2 0 7 】

(付記 2 3) 該口座から減額した現金を、該決済サービス提供者が一時的に保持しておき、

該受給者が該有価データの現金化を該決済サービス提供者に許可した場合、該決済サービス提供者は、前記所有権移転ステップを実行する一方、

該受給者が該有価データの無効化を該決済サービス提供者に依頼した場合、該決済サービス提供者は、一時的に保持されていた現金を該口座に戻すことを特徴とする、付記 2 2 記載の電子決済方法。

【 0 2 0 8 】

(付記 2 4) 該受給者が該有価データの無効化を該決済サービス提供者に依頼した場合、該決済サービス提供者は、該電子情報本体の所有者である該供給者から該有価データの無効化の承認を得た後、一時的に保持されていた現金を該口座に戻すことを特徴とする、付記 2 3 記載の電子決済方法。

(付記 2 5) 該受給者は、該決済サービス提供者と予め契約しておき、

前記添付ステップで有価データを該電子情報本体に添付した場合、該決済サービス提供者が、添付した有価データに対応する金額を立て替えることを特徴とする、付記 1 ～付記 2 1 のいずれか一つに記載の電子決済方法。

【 0 2 0 9 】

(付記 2 6) 正規の受取人以外の利用者によって利用可能な該電子情報本体の機能が、該電子情報本体に有価データを添付・追加する機能に限定されていることを特徴とする、付記 1 ～付記 2 5 のいずれか一つに記載の電子決済方法。

(付記 2 7) 該決済サービス提供者が、前記添付ステップにおいて該電子情報本体に有価データを添付・追加する都度、該電子情報本体と追加された有価データとを含む部分に対する電子署名を作成して、該有価データ搬送用電子情報に添付することを特徴とする、付記 2 6 記載の電子決済方法。

【 0 2 1 0 】

(付記 2 8) 該決済サービス提供者が、該電子情報本体と、電子署名によって該電子情報本体に既に連結されている有価データと、該追加された有価データとの全てに対する電子署名を作成して、該有価データ搬送用電子情報に添付することを特徴とする、付記 2 7 記載の電子決済方法。

(付記 2 9) 該決済サービス提供者が、該電子情報本体と該追加された有価データとに対する電子署名を作成して、該有価データ搬送用電子情報に添付することを特徴とする、付記 2 7 記載の電子決済方法。

【 0 2 1 1 】

(付記 3 0) 該電子情報本体に、該電子情報本体の発行者による電子署名が添付されていることを特徴とする、付記 1 ～付記 2 9 のいずれか一つに記載の電子決済方法。

(付記 3 1) 該受給者が、追加情報を該電子情報本体に追加した場合、該電子情報本体と該追加情報とに対する電子署名を作成して、該電子情報本体に添付することを特徴とする、付記 1 ～付記 3 0 のいずれか一つに記載の電子決済方法。

【 0 2 1 2 】

(付記 3 2) 前記添付ステップで該電子情報本体に添付される有価データを所定の公開鍵により暗号化し、該所定の公開鍵に対応する秘密鍵を、該決済サービス提供者および前記受取人のうちの少なくとも一方が管理することを特徴とする、付記 1 ～付記 3 1 のいずれか一つに記載の電子決済方法。

(付記 3 3) 前記添付ステップで該電子情報本体に添付される有価データを所定の公開鍵により暗号化し、前記受取人が、該所定の公開鍵に対応する秘密鍵を記録された可搬型記録媒体を保持することを特徴とする、付記 1 ～付記 3 1 のいずれか一つに記載の電子決済方法。

【 0 2 1 3 】

(付記 3 4) 該所定の公開鍵が、該電子情報本体に記録されていることを特徴とする、付記 3 2 または付記 3 3 に記載の電子決済方法。

(付記 3 5) 該所定の公開鍵が、信用機関から取得されることを特徴とする、付記 3 2 または付記 3 3 に記載の電子決済方法。

(付記 3 6) 前記添付ステップで該電子情報本体に添付される有価データに、該決済サービス提供者による電子署名が添付されていることを特徴とする、付記 1 ～付記 3 5 のいずれか一つに記載の電子決済方法。

【 0 2 1 4 】

(付記 3 7) 前記所有権移転ステップにおいて、該有価データを現金化し、該有価データに対応する現金を所定の口座に振り込むことを特徴とする、付記 1 ～付記 3 6 のいずれか一つに記載の電子決済方法。

(付記 3 8) 前記所有権移転ステップにおいて、該有価データを現金化し、該有価データに対応する現金を、該有価データの受取人本人であると認証された前記受取希望者に手渡すことを特徴とする、付記 1 ～付記 3 6 のいずれか一つに記載の電子決済方法。

【 0 2 1 5 】

(付記 3 9) 該決済サービス提供者が発行した全ての有価データのそれぞれに固有の識別子が付与され、市場に流通している有価データの識別子のみが該決済サービス提供者によって保持されることを特徴とする、付記 1 ～付記 3 8 のいずれか一つに記載の電子決済方法。

(付記 4 0) 前記所有権移転ステップにおいて、該有価データに付与された識別子が該決済サービス提供者によって保持されている場合に、該有価データの所有権が当該受取希望者に移転されることを特徴とする、付記 3 9 記載の電子決済方法。

【 0 2 1 6 】

(付記 4 1) 該電子情報本体に任意のデータが添付されることを特徴とする、付記 1 ～付記 4 0 のいずれか一つに記載の電子決済方法。

(付記 4 2) 前記任意のデータとして、日付、時刻、該受給者の名前、該

受給者の住所，該受給者の電話番号，該受給者の電子メールアドレス，前記対価の支払い理由，前記対価の金額，前記商取引で取り扱われる商品の発送先，該受給者所有の有価データ搬送用電子情報本体のうちの少なくとも一つが添付されることを特徴とする、付記41記載の電子決済方法。

## 【0217】

（付記43） 該供給者は、該供給者所有の電子情報本体を一般公開し、前記取得ステップにおいて、該受給者が、一般公開された該電子情報本体を取得することを特徴とする、付記1～付記42のいずれか一つに記載の電子決済方法。

## 【0218】

（付記44） 該決済サービス提供者は、支払可能額情報を有する電子小切手帳を該受給者に予め発行し、

前記依頼ステップにおいて、該受給者が、前記商取引に必要な対価に対応する価値を有する有価データを該電子情報本体に添付するように該決済サービス提供者に依頼する際、該電子小切手帳を該電子情報本体とともに送信し、

前記添付ステップにおいて、該決済サービス提供者が、該有価データを該電子情報本体に添付した場合、該電子小切手帳の該支払可能額情報から該有価データの価値に応じた額を減額した支払可能額情報を有する新たな電子小切手帳を作成し、該新たな電子小切手帳を該受給者に返送することを特徴とする、付記1～付記44のいずれか一つに記載の電子決済方法。

## 【0219】

なお、該受給者の依頼に応じて、一つの該電子情報本体に、2以上の異なる決済サービス提供者によって2以上の有価データが発行されて添付されてもよく、このとき、該異なる決済サービス提供者によって該2以上の有価データが該電子情報本体に添付されている場合、前記所有権移転ステップで該有価データの所有権の移転を行なう該決済サービス提供者は、各有価データの発行元である決済サービス提供者から、各有価データに対応する現金を集金してもよい。

また、該電子情報本体に添付される該有価データが、電子通貨、電子証券、電子チケットおよび電子許可証のうちの少なくとも一つの機能を有するものとし、

一つの該電子情報本体に、2以上の異なる種類の有価データを添付してもよい。

#### 【0220】

一方、前記商取引により該供給者から該受給者に受け渡されるべき商品が電子チケットもしくは電子許可証である場合、該供給者が、前記返送ステップで該有価データ搬送用電子情報を受け取ると、該受給者所有の有価データ搬送用電子情報本体に前記の電子チケットもしくは電子許可証を添付し、その電子情報本体を該受給者に送付してもよく、このとき、前記返送ステップで該有価データ搬送用電子情報が該受給者経由で返送され、該電子情報が該受給者を経由した際に、該受給者により、該受給者所有の有価データ搬送用電子情報本体が、該決済サービス提供者から該供給者へ返送される該有価データ搬送用電子情報に添付されて、該供給者へ受け渡される。また、このとき、該受給者は、前記の電子チケットもしくは電子許可証を添付された電子情報本体を受け取り、前記の電子チケットもしくは電子許可証の内容を提示して前記の電子チケットもしくは電子許可証を利用してもよいし、さらに、該受給者は、前記の電子チケットもしくは電子許可証を添付された電子情報本体を携帯情報端末で受け取り、前記の電子チケットもしくは電子許可証の内容を該携帯情報端末の表示部に表示させてもよい。

#### 【0221】

##### 【発明の効果】

以上詳述したように、本発明の電子決済方法（請求項1～5）によれば、以下のような効果ないし利点を得ることができる。

〔1〕供給者、受給者、決済サービス提供者の間で、供給者所有の有価データ搬送用電子情報本体（電子財布）をやり取りすることにより、受給者は、決済サービス提供者を介して供給者に商取引に必要な対価を電子的に支払うことができる。このとき、受給者は、直接、供給者への代金の支払いをコントロールすることができるので、受給者が安心して決済を行なえ、インターネット等を利用した電子商取引を活発化させ売上を大幅に向上させることができる（請求項1，付記1）。

#### 【0222】

〔2〕決済サービス提供者が受給者の依頼に応じて有価データを発行すること

により、決済サービス提供者が、市場に流通している有価データを全て把握することができ、システムのセキュリティを維持する仕組み（二重使用防止システム）を簡素化できそのシステムを安価に構築することができる（請求項1，付記1）。

【0223】

〔3〕 決済サービス提供者が受給者の依頼に応じて有価データを電子情報本体に添付するので、供給者のシステムを一切介在させることなく、決済が行なわれる。また、供給者が決済サービス提供者に取引内容を通知する必要が無くなる。従って、供給者が操作ミスにより請求金額を誤ったり、供給者の不正行為（詐欺等）により受給者が現金を奪われたりすることを一切排除できる。また、現金移動時にクレジットカード番号、パスワードなどの秘密情報が供給者に漏れることもなくなるとともに、その秘密情報がインターネット等のネットワーク上で盗聴・盗難に遭うこともなくなる（請求項1，付記1）。

【0224】

〔4〕 供給者が決済サービス提供者に取引内容を通知する必要がなく、電子情報本体に添付された有価データに受給者の情報が含まれておらず、さらに、電子小切手のごとく電子署名に受給者の署名を使用しないので、受給者のプライバシーが確実に保護される（請求項1，付記1）。

【0225】

〔5〕 供給者は、決済サービス提供者から返送されてきた、有価データを添付された電子情報を受け取るので、即座に入金金額を確認することができ、商品発送までの時間を短縮することができる。また、入金通知処理も自動化することができるほか、受給者との取引の度にクレジット会社等と通信する必要が無くなるため、自動化システム構築のコストを低く抑えることができる（請求項1，付記1）。

【0226】

〔6〕 電子情報本体に添付された有価データの現金化（所有権の移転）は、その電子情報本体に予め登録された受取人本人しか行なえないので、万一、有価データを含む電子情報が盗難されたり複製されたりして、受取人本人以外が有価デ

ータを現金化しようとしても、現金化を行なうことができない。従って、不正な現金化を確実に阻止することができる（請求項1，付記1）。

【0227】

〔7〕電子情報本体に、この電子情報本体の発行元に関する発行元情報を外部から確認可能に記録しておくことにより、電子情報本体（電子財布）の発行元を誰でも確認することができる。これにより、その電子情報本体に添付された有価データを必ず現金化できることが保証され、利用者（受給者，供給者）に安心感を与えることができる（付記2）。

【0228】

〔8〕電子情報本体に有価データを外部から確認可能に添付することにより、有価データを添付された電子情報本体を決済サービス提供者から供給者へ返送する際に、その電子情報を受け取った者（受給者，第三者，供給者）は誰でも有価データの内容（入金金額等）を確認することができる（付記3）。

【0229】

〔9〕有価データを添付された電子情報本体を、決済サービス提供者から受給者経由で供給者へ返送することにより、電子情報が供給者に返送される前に、受給者が、支払い金額を最終的に確認し、入金金額が正しいかどうかを判断することができる。このとき、供給者は、受給者から直接、有価データ付きの電子情報を受け取るので、即座に入金金額を確認することができ、商品発送までの時間を大幅に短縮することができる（付記4）。

【0230】

〔10〕有価データを添付された電子情報本体を、決済サービス提供者から、予め登録された受給者以外の一以上の第三者経由で供給者へ返送することにより、電子情報が供給者に返送される前に、第三者が、支払い金額を最終的に確認し、入金金額が正しいかどうかを判断することができる。これは、受給者と実際の対価の支払い者とが異なる場合などのように購入の承認者が他に存在する場合に有効である。また、支払い者が受給者とは独立に商取引内容をチェックできるので、例えば受給者に成りすまして行なわれた商取引に伴う、予期せぬ支払いの発生を監視し、その支払いの実行を確実に阻止することができる（付記5）。



【0231】

〔11〕有価データ搬送用電子情報の返送先／経由先を決済サービス提供者側に予め登録しておき、その電子情報を、決済サービス提供者から、予め登録された返送先／経由先へ返送することにより、電子情報の返送先／経由先を不正に変更することは難しくなる。従って、受給者は安心して電子情報本体に対する入金（有価データの添付）を行なえる。また、供給者に電子情報が直接返送される場合、供給者に確実に電子情報が返却されるので、電子情報が第三者に渡って不正に現金化されたり商取引の邪魔をされたりすることがなくなり、受給者は安心して供給者に現金を支払うことができる（付記6，8）。

【0232】

〔12〕有価データ搬送用電子情報の返送先／経由先をその電子情報に予め記録しておき、その電子情報を、決済サービス提供者から、予め記録された返送先／経由先へ返送することにより、利用者（受給者，供給者，第三者）は、電子情報の行き先を自分で確認することができる。また、供給者に電子情報が直接返送される場合、受給者は、支払い先が明確になり安心感を得ることができるほか、供給者は、電子情報が必ず自分の所に帰ってくるかどうかを確認することができる（付記7，9）。

【0233】

〔13〕電子情報本体に記録された認証用情報を、受取希望者の認証時にこの受取希望者から取得された認証対象情報と照合されるべき受取人認証情報とすることにより、受取人と電子情報本体との確実な対応関係を築くことができ、電子情報本体における匿名性を維持しながら受取人本人のみが有価データを現金化することができる。また、電子情報本体中に受取人認証情報を記録するため、受取人認証情報の管理をするためのシステムが不要である（付記10）。

【0234】

〔14〕電子情報本体を決済サービス提供者によって発行し、電子情報本体固有の識別子を認証用情報として電子情報本体に予め記録するとともに、受取希望者の認証時にこの受取希望者から取得された認証対象情報と照合されるべき受取人認証情報を、上記識別子に対応付けて、決済サービス提供者が保持しておくこ

とにより、電子情報本体における匿名性を維持しながら受取人本人のみが有価データを現金化することができる。特に、この場合、受取人認証情報は決済サービス提供者側で保持され、電子情報本体には識別子が記録されるだけなので、受取人認証情報の書換による不正な現金化を確実に阻止することができる（付記 1 1）。

【 0 2 3 5 】

〔 1 5 〕 電子情報本体を決済サービス提供者によって発行し、電子情報本体固有の識別子を認証用情報として電子情報本体に予め記録するとともに、受取希望者の認証時にその受取希望者から取得された認証対象情報と照合されるべき受取人認証情報を、上記識別子に対応付けて、可搬型記録媒体に記録しておくことにより、その可搬型記録媒体を電子情報本体の受取人が所持・管理することができ、決済サービス提供者側での受取人認証情報の管理が不要となる。また、バイオメトリクス情報を受取人認証情報として用いる場合、その受取人認証情報のプライバシーを自分自身で管理することができる（付記 1 2）。

【 0 2 3 6 】

〔 1 6 〕 受取人認証情報として文字列を用いることにより、従来広く用いられているパスワード方式による本人認証と同じ方式を採用することができ、本人認証方式が利用者に受け入れられやすい（付記 1 3）。

〔 1 7 〕 受取人認証情報として受取人本人のバイオメトリクス情報を用いることにより、受取人の本人認証が確実に行なえるようになり、安全性が高まる。また、パスワードのように受取人が受取人認証情報を記憶する必要がなく、受取人認証情報の管理を特別に行なう必要がない（付記 1 4）。

【 0 2 3 7 】

〔 1 8 〕 受取人を、電子情報本体の所有者、もしくは、供給者を管理する管理者とし、受取人認証情報として、その所有者もしくは管理者の認証情報を登録することにより、所有者もしくは管理者と電子情報本体との確実な対応関係を築くことができ、有価データの現金化は、所有者もしくは管理者以外は無価値データを現金化することができなくなる（付記 1 5, 1 6）。

【 0 2 3 8 】

〔19〕受給者、供給者および決済サービス提供者の相互間の情報転送を有線通信手段や無線通信手段のうちの少なくとも一方によって行なうことで、即時性が高くなり、快適に電子決済システムを利用することができる（付記17）。

〔20〕受給者、供給者および決済サービス提供者の相互間の情報転送を、可搬型記録媒体をやり取りすることによって行なうことで、オフラインでも電子決済を使用でき、通信環境を整える必要が無くなる（付記18）。

【0239】

〔21〕決済サービス提供者が、受給者や予め登録された第三者を含む確認先に対し、有価データ添付の実行確認を行なうことにより、不正な現金移動が実行されようとしている場合にその事実が事前に判明し、不正な現金移動を未然に防止することができるので、安全性をより高めることができる（付記19）。その際、確認先を決済サービス提供者側に予め登録しておけば、不正な現金移動を発覚させないよう犯罪者等が確認先を書き換えることが困難になる（付記20）。また、確認先を有価データ搬送用電子情報に随時記録すれば、その電子情報を使用する度に現金移動の確認先を柔軟に変更することができる（付記21）。

【0240】

〔22〕決済サービス提供者側における受給者の口座に現金を予め入金しておき、決済サービス提供者が、電子情報本体に添付した有価データに対応する金額をその口座から減額することにより、決済サービス提供者は、受給者から予め預かっておいた現金を用いて、電子情報本体に対する入金処理を行なうことができるので、受給者からの集金の手間が省けるとともに、受給者から入金金額に対応する現金を回収できなくなるというリスクも無くなる（付記22）。

【0241】

〔23〕受給者の口座から減額した現金を決済サービス提供者が一時的に保持しておき、決済サービス提供者は、受給者からの許可を受けて有価データの現金化を行なう一方、受給者が許可しない場合には、一時的に保持されていた現金を受給者の口座に戻すようにすることで、決済サービス提供者は、受給者と供給者との間の商取引に対し、エスクローサービス（第三者仲介）を提供することができる（付記23）。

## 【 0 2 4 2 】

〔 2 4 〕 受給者が有価データの無効化を決済サービス提供者に依頼した場合、決済サービス提供者は、供給者から有価データの無効化の承認を得た後、一時的に保持されていた現金を受給者の口座に戻すことにより、決済サービス提供者が預かっていた現金は、受給者および供給者の両者からの承認が得られないと受給者の口座には戻らず、供給者の安全性も守られるようになる（付記 2 4）。

## 【 0 2 4 3 】

〔 2 5 〕 受給者は、決済サービス提供者と予め契約しておき、決済サービス提供者が、電子情報本体に添付した有価データに対応する金額を立て替え、後日、立て替えた金額を受給者に請求することで、受給者は、残金を気にすることなく電子情報本体に入金でき、受給者にとって便利になる。また、この方法は、従来のクレジットカードサービスと同じ仕組みであるので、既存のクレジットカードサービスシステムをそのまま使用することができる（付記 2 5）。

## 【 0 2 4 4 】

〔 2 6 〕 正規の受取人以外の利用者が利用できる電子情報本体の機能を、電子情報本体に有価データを添付・追加する機能のみに限定することにより、決済サービス提供者が市場に流通している有価データを全て管理可能であること、および、受取人本人以外が有価データを現金化することができないことと相俟って、セキュリティ維持（複製防止、二重使用防止）のためのシステム構築がほとんど不要となる。逆に有価データを含む電子情報を複製して自由にバックアップできる環境を利用者に提供することができ、利用者は多大な安心感を得ることができる。また、有価データを添付された電子情報について複製防止技術が不要になるため、その電子情報を電子メールに添付するなどして受給者、供給者、決済サービス提供者の相互間で極めて簡単にやり取りすることができる（請求項 2，付記 2 6）。

## 【 0 2 4 5 】

〔 2 7 〕 決済サービス提供者が、電子情報本体に有価データを添付・追加する都度、電子情報本体と追加された有価データとを含む部分に対する電子署名を作成して、有価データ搬送用電子情報に添付することにより、有価データのみを電

子情報から不正に取り出すことは不可能で、電子情報本体に添付された有価データを第三者が不正に現金化することはできない（請求項 3，付記 2 7～2 9）。

【 0 2 4 6 】

〔 2 8 〕 電子情報本体に、その電子情報本体の発行者による電子署名を添付したり、受給者が、追加情報を電子情報本体に追加した場合、電子情報本体と追加情報とに対する電子署名を作成して電子情報本体に添付したりすることにより、第三者が、電子情報本体に記録されている各種情報を改竄することができなくなり、安全性が高まる（付記 3 0， 3 1）。

【 0 2 4 7 】

〔 2 7 〕 電子情報本体に添付される有価データを所定の公開鍵により暗号化し、その公開鍵に対応する秘密鍵を、決済サービス提供者および受取人のうちの少なくとも一方が管理することにより、有価データを正しく復号化するには、秘密鍵が必要になるので、有価データを実体化（現金化）できるのは、決済サービス提供者もしくは受取人（電子情報本体の所有者や管理者等）に限定される（請求項 4，付記 3 2）。

【 0 2 4 8 】

〔 3 0 〕 電子情報本体に添付される有価データを所定の公開鍵により暗号化し、受取人（電子情報本体の所有者や管理者等）が、その公開鍵に対応する秘密鍵を記録された可搬型記録媒体を保持することにより、有価データの読出し即ち現金化は、秘密鍵を記録した記録媒体の所持者（受取人）しか行なえなくなる（付記 3 3）。

【 0 2 4 9 】

〔 3 1 〕 所定の公開鍵を電子情報本体に記録しておけば、電子情報本体に対する入金処理を行なう決済サービス提供者は、即座に公開鍵を入手して有価データを暗号化することができる。その際、電子情報本体に電子署名を施しておけば、公開鍵を改竄することができないので、安全性を確保することができる（付記 3 4）。

〔 3 2 〕 所定の公開鍵を信用機関から随時取得することにより、第三者による公開鍵の書き換えが難しくなり、安全性が高まる（付記 3 5）。

【0250】

〔33〕電子情報本体に添付される有価データに、決済サービス提供者による電子署名を添付することにより、有価データの発行元である決済サービス提供者以外の者による有価データの書換えを阻止することができる（付記36）。

〔34〕決済サービス提供者が、有価データを現金化した際に現金を所定の口座に振り込むことにより、受取人本人（電子情報本体の所有者・管理者）は、銀行窓口まで行くことなく、WEBなどを使用してオンラインで現金化を行なえ便利である（付記37）。

【0251】

〔35〕決済サービス提供者が、有価データを現金化した際に現金を受取人本人であると認証された受取希望者に手渡すことにより、受取人は、前もって口座を開いておく必要が無く、手間がかからない（付記38）。

〔36〕決済サービス提供者が発行した全ての有価データのそれぞれに固有の識別子を付与し、市場に流通している有価データの識別子のみを決済サービス提供者によって保持することにより、市場に流通している有価データの内、決済サービス提供者が発行したものを全て把握することができる。このとき、現金化対象の有価データに付与された識別子が決済サービス提供者によって保持されている場合に、その有価データの所有権を受取希望者に移転するようにする。これにより、二重現金化のチェックを安価なシステムで実現できるほか、偽造有価データの発見も極めて簡単に行なえる（付記39，40）。

【0252】

〔37〕電子情報本体に、任意のデータ（例えば日付，時刻，受給者の名前，受給者の住所，受給者の電話番号，受給者の電子メールアドレス，対価の支払い理由，対価の金額，商取引で取り扱われる商品の発送先，受給者所有の有価データ搬送用電子情報本体のうちの少なくとも一つ）を添付することにより、受給者が供給者に発注内容などを別便で送付する必要がなくなり利用者（受給者や供給者）の利便性が高まるほか、電子情報内の入金内容と発注内容との対応関係が明確になり供給者の管理が楽になる（付記41，42）。

【0253】

〔38〕供給者所有の電子情報本体を一般公開し、受給者が、一般公開された電子情報本体を取得できるようにすることで、受給者が必要なときに電子情報本体を取得して発注処理を行なうことができる。つまり、供給者が各受給者と個別に対応をとって電子情報本体を受給者に与える必要が無くなる（付記43）。

## 【0254】

〔39〕決済サービス提供者は、支払可能額情報を有する電子小切手帳を受給者に予め発行し、受給者は、電子小切手帳を電子情報本体に添付して決済サービス提供者に送信し、その電子小切手帳によって商取引に必要な対価の支払いを行なうようにする。このとき、電子小切手帳には、常に受給者が支払える限度額（支払可能額情報）が記録されており、受給者は、随時、その限度額を確認することができる。つまり、受給者は常に手元で素早く残高を確認できる。従って、受給者はわざわざ決済サービス提供者にアクセスして口座の残高を確認したり、残高を自分で覚えておいたりする必要がなくなり、受給者の利便性をより高めることができる（付記44）。

## 【0255】

〔40〕受給者の依頼に応じて、一つの電子情報本体に、2以上の異なる決済サービス提供者によって2以上の有価データを発行して添付する。そして、その2以上の有価データを現金化する際、決済サービス提供者は、各有価データの発行元である決済サービス提供者から、各有価データに対応する現金を集金する。これにより、供給者と受給者との間の商取引の柔軟性が増し、供給者および受給者の双方とも便利になる。このように一つの電子情報本体に複数の金融機関の小切手等を持たせることができると、電子情報本体の使い勝手は通常の電子マネーと同じになり、通常の電子マネーと変わらない利便性（匿名性、誰でも使える環境）を利用者に提供することができる。また、電子財布の発行元が各決済サービス提供者と協調して各有価データを現金化するので、受取人は、複数の決済サービス提供者と交渉する必要が無くても済む。

## 【0256】

〔41〕電子情報本体に添付される有価データを、電子通貨、電子証券、電子チケットおよび電子許可証のうちの少なくとも一つの機能を有するものとすれば

、各種有価データを受給者、供給者、決済サービス提供者の相互間で安全に搬送することができる。また、一つの電子情報本体に、2以上の異なる種類の有価データを添付することにより、受給者や電子財布の所有者は複数の電子情報本体を使い分ける必要が無くなり、受給者や電子財布の所有者の利便性をより高めることができる。

【0257】

〔42〕供給者が電子チケットや電子許可証を受給者所有の電子情報本体に添付して受給者に送付することにより、確実かつ安全に商品を受給者に受け渡すことができる。その際、決済サービス提供者から供給者へ返送される供給者所有の電子情報が受給者を経由した際に、その供給者所有の電子情報に受給者所有の電子情報本体を添付することで、受給者は、極めて容易に供給者に受給者所有の電子情報本体を受け渡すことができる。また、受給者は、電子チケットや電子許可証を添付された電子情報本体を受け取ると、電子チケットや電子許可証の内容を提示することにより電子チケットや電子許可証を利用することができ、特に、電子チケットや電子許可証を添付された電子情報本体を携帯情報端末で受け取った場合、その電子チケットや電子許可証の内容を携帯情報端末の表示部に表示させて係員等に示すだけで、極めて容易に電子チケットや電子許可証を利用することができる。

【図面の簡単な説明】

【図1】

本発明の第1実施形態としての電子決済方法を適用されるシステムの構成および同方法の手順を説明するための図である。

【図2】

第1実施形態の電子財布本体に対する電子署名付与手法および情報追加手法の第1例を説明するための図である。

【図3】

第1実施形態の電子財布本体に対する電子署名付与手法および情報追加手法の第2例を説明するための図である。

【図4】



第 1 実施形態における電子財布への有価データの追加・保存手法の第 1 例を説明するための図である。

【図 5】

第 1 実施形態における電子財布への有価データの追加・保存手法の第 2 例を説明するための図である。

【図 6】

第 1 実施形態における電子財布への有価データの追加・保存手法の第 2 例を説明するための図である。

【図 7】

第 1 実施形態における電子財布への有価データの追加・保存手法の第 3 例を説明するための図である。

【図 8】

第 1 実施形態における電子財布への有価データの追加・保存手法の第 3 例を説明するための図である。

【図 9】

本発明の第 2 実施形態としての電子決済方法を適用されるシステムの構成および同方法の手順を説明するための図である。

【図 1 0】

第 2 実施形態における電子チケット（電子許可証）の利用手法を説明するための図である。

【符号の説明】

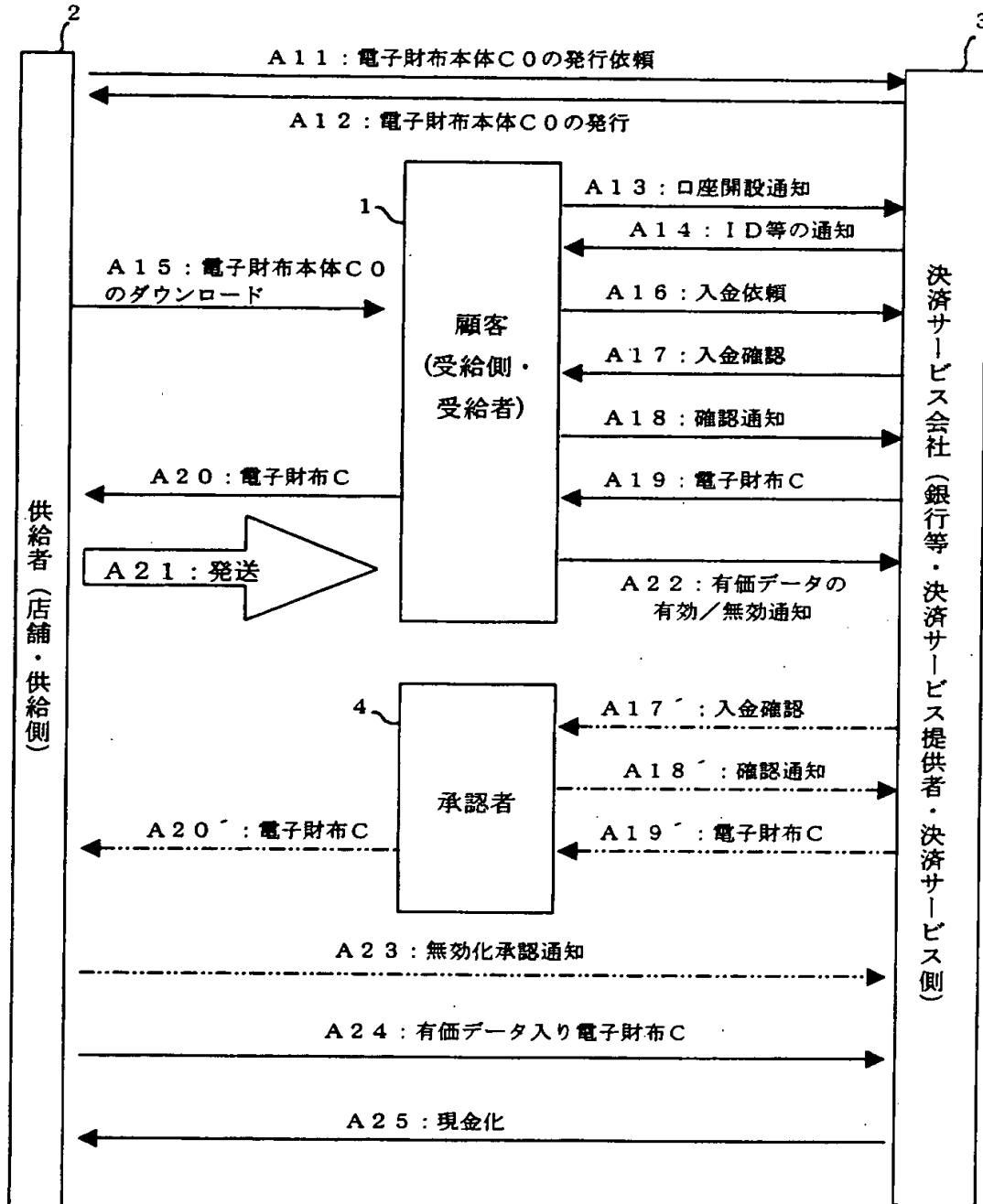
- 1 顧客（受給者，受給側，受給側端末）
- 2 店舗（供給者，供給側，供給側サーバ，チケット販売会社）
- 3 決済サービス会社（決済サービス提供者，決済サービス側，決済サービス側サーバ）
- 4 承認者（第三者，承認者端末）
- 5 会場
- 1 0 携帯電話（携帯情報端末）
- 1 1 表示部

C, K 電子財布 (有価データ搬送用電子情報)

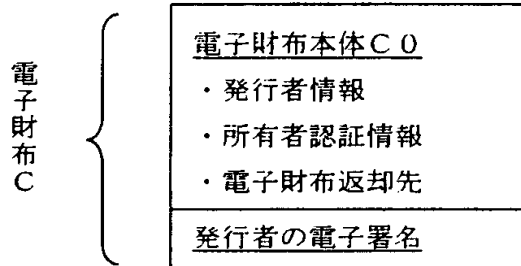
C 0, K 0 電子財布本体 (有価データ搬送用電子情報本体)

【書類名】 図面

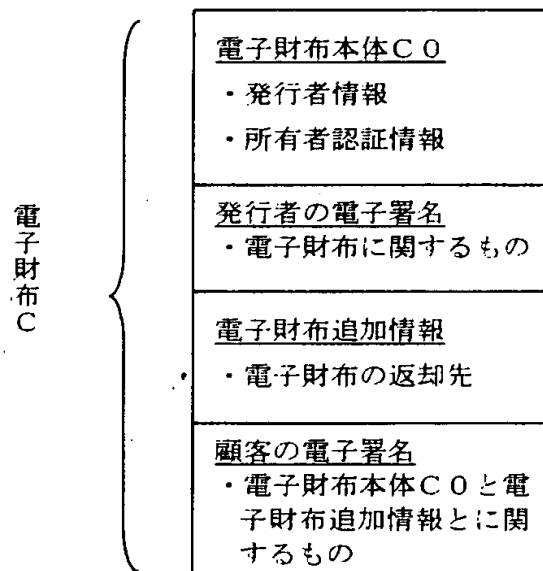
【図 1】



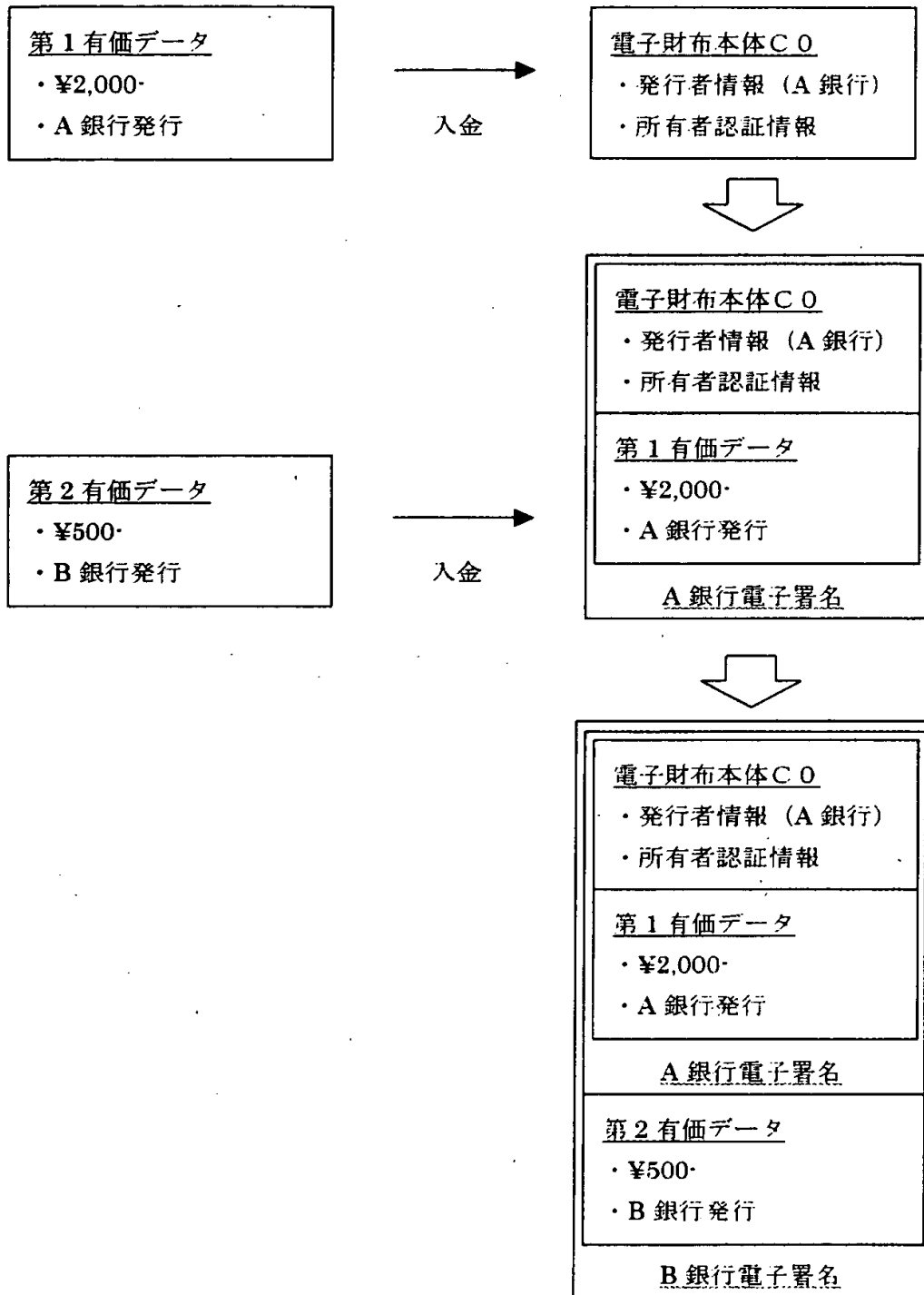
【図 2】



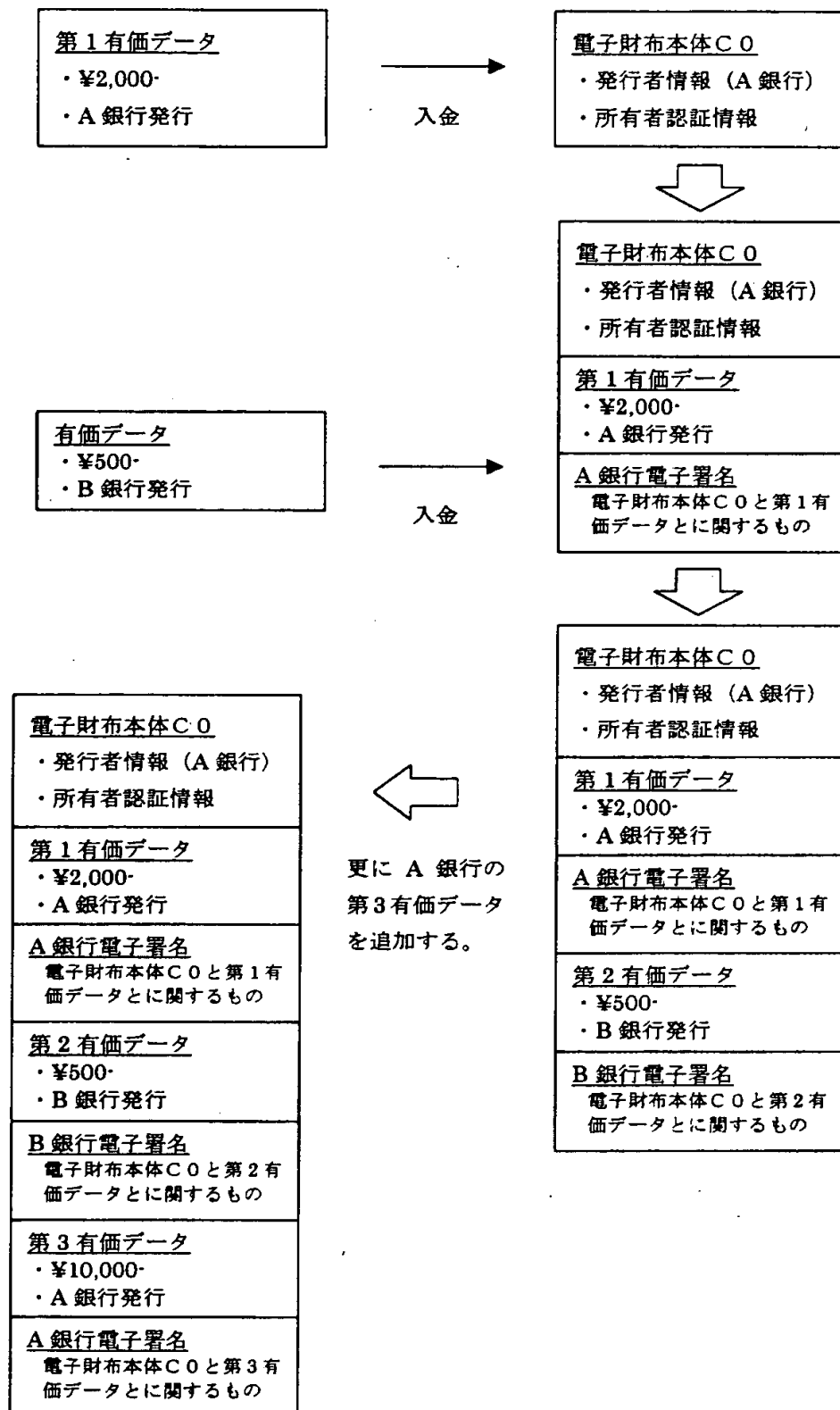
【図 3】



【図 4】



【図 5】



【図 6】

<u>電子財布本体 C 0</u> ・ 発行者情報 (A 銀行) ・ 所有者認証情報
<u>第 2 有価データ</u> ・ ¥500 ・ B 銀行発行
<u>B 銀行電子署名</u> 電子財布本体 C 0 と第 2 有 価データとに関するもの

【図 7】

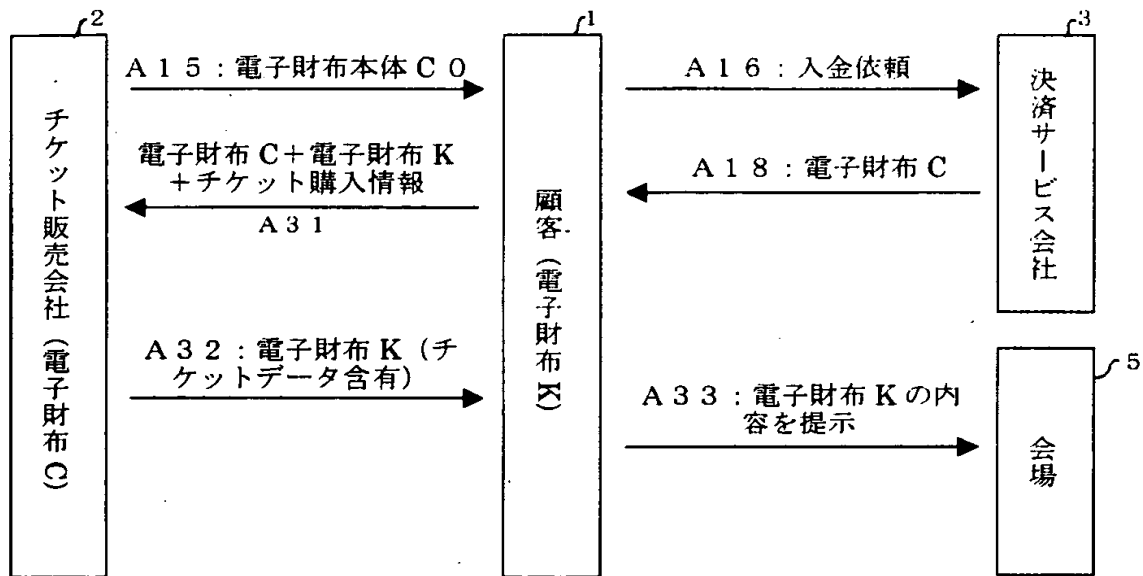
<u>電子財布本体 C 0</u> ・ 発行者情報 (A 銀行) ・ 所有者認証情報 ・ 暗号化公開鍵
<u>有価データ</u> ・ ¥500 ・ B 銀行発行
<u>B 銀行電子署名</u> 有価データに関するもの
公開鍵で暗号化

【図 8】

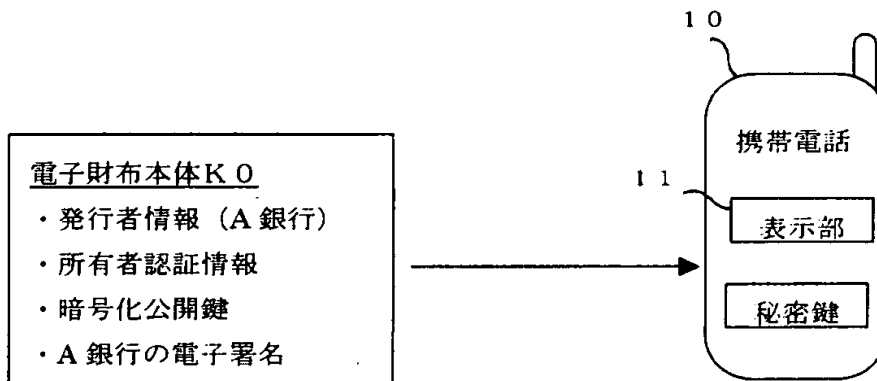
<p><u>電子財布本体 C 0</u></p> <ul style="list-style-type: none"> <li>・ 発行者情報 (A 銀行)</li> <li>・ 所有者認証情報</li> <li>・ 暗号化公開鍵</li> </ul>
<p><u>第 1 有価データ</u></p> <ul style="list-style-type: none"> <li>・ ¥500・</li> <li>・ B 銀行発行</li> </ul>
<p><u>B 銀行電子署名</u></p> <p>第 1 有価データに関するもの</p>
<p>公開鍵で暗号化</p>
<p><u>第 2 有価データ</u></p> <ul style="list-style-type: none"> <li>・ ¥500・</li> <li>・ A 銀行発行</li> </ul>
<p><u>A 銀行電子署名</u></p> <p>第 2 有価データに関するもの</p>
<p>公開鍵で暗号化</p>



【図9】



【図10】



【書類名】            要約書

【要約】

【課題】 商取引の手順を工夫することにより受給者が安心して決済を行なえるようにして、電子商取引の活発化、ひいては売上向上を実現するとともに、二重使用防止システムを簡易かつ安価に構築できるようにする。

【解決手段】 受給者 1 が、供給者 2 所有の電子財布本体 C 0 を取得してから、決済サービス提供者 3 に対して電子情報本体 C 0 を送信するとともに有価データを電子財布本体 C 0 に添付するように依頼し、決済サービス提供者 3 が、受給者 1 の依頼に応じて、受給者 1 の認証後、有価データを電子情報本体 C 0 に添付し、電子情報本体 C 0 と有価データとからなる電子財布 C を供給者 2 へ返送し、電子財布 C における有価データの受取希望者が電子情報本体 C 0 における認証用情報に基づいて有価データの受取人本人であると認証された場合に限り、決済サービス提供者 3 によって、有価データの所有権を当該受取希望者に移転する。

【選択図】            図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社